

# Lessons From The Legion

Nick Drage

Path Dependence Limited

DevSecCon - 19 Oct 18

V 4.11 - 19Oct



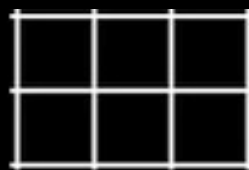
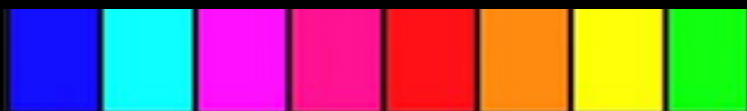
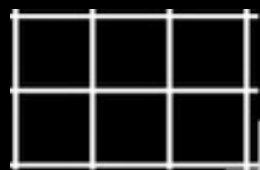
DevSecCon

# Lessons From the Legion ( The DevSecCon Remix )

NICK DRAGE



LONDON 18-19 OCT  
2018

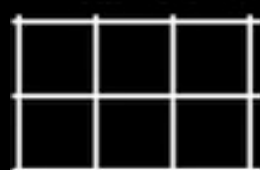


TCG +00:00:00:00

EARLY (23.98 fps)

LATE (23.98 fps)

12 11 10 9 8 7 6 5 4 3 2 1 0 1 2 3 4 5 6 7 8 9 10 11 1





DevSecCon

# Lessons From the Legion ( The DevSecCon Remix )

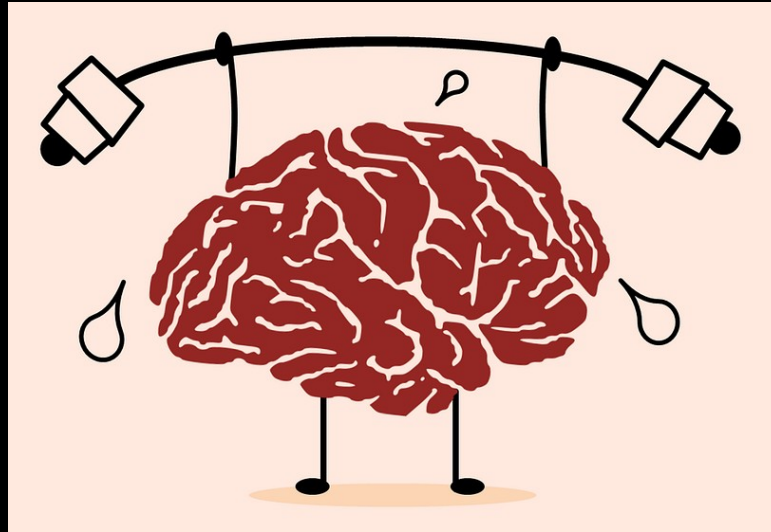
NICK DRAGE



LONDON 18-19 OCT  
2018



# I have a question



# You'll Have Questions...

- Available afterwards
- Contact details at the end
- All references blogged
- All media – owner's copyright
- If no credit, probably Pixabay





Nick Drage – Path Dependence – @SonOfSunTzu





# ***Win the Cyberwar With Zero Trust***

John Kindervag

*Field CTO*



## *The Four Levels of War*

**Grand Strategy  
(Political)**

**The Ultimate Goal**

**Strategy**

**The Big Idea**

**Tactics**

**The Things You Use**

**Operations**

**The Way You Use Them**

## *The Four Levels of Cyberwar*

**Grand Strategy  
(Political)**

**Stop Data  
Breaches**

**Strategy**

**Zero Trust**

**Tactics**

**Tools/Policies**

**Operations**

**Platform**

## *The Four Levels of Cyberwar*

**Grand Strategy  
(Political)**

**The Ultimate Goal**

**Strategy**

**The Big Idea**

**Tactics**

**The Things You Use**

**Operations**

**The Way You Use Them**



# Tactics

- System Administrators
- Developers
- Security Operations

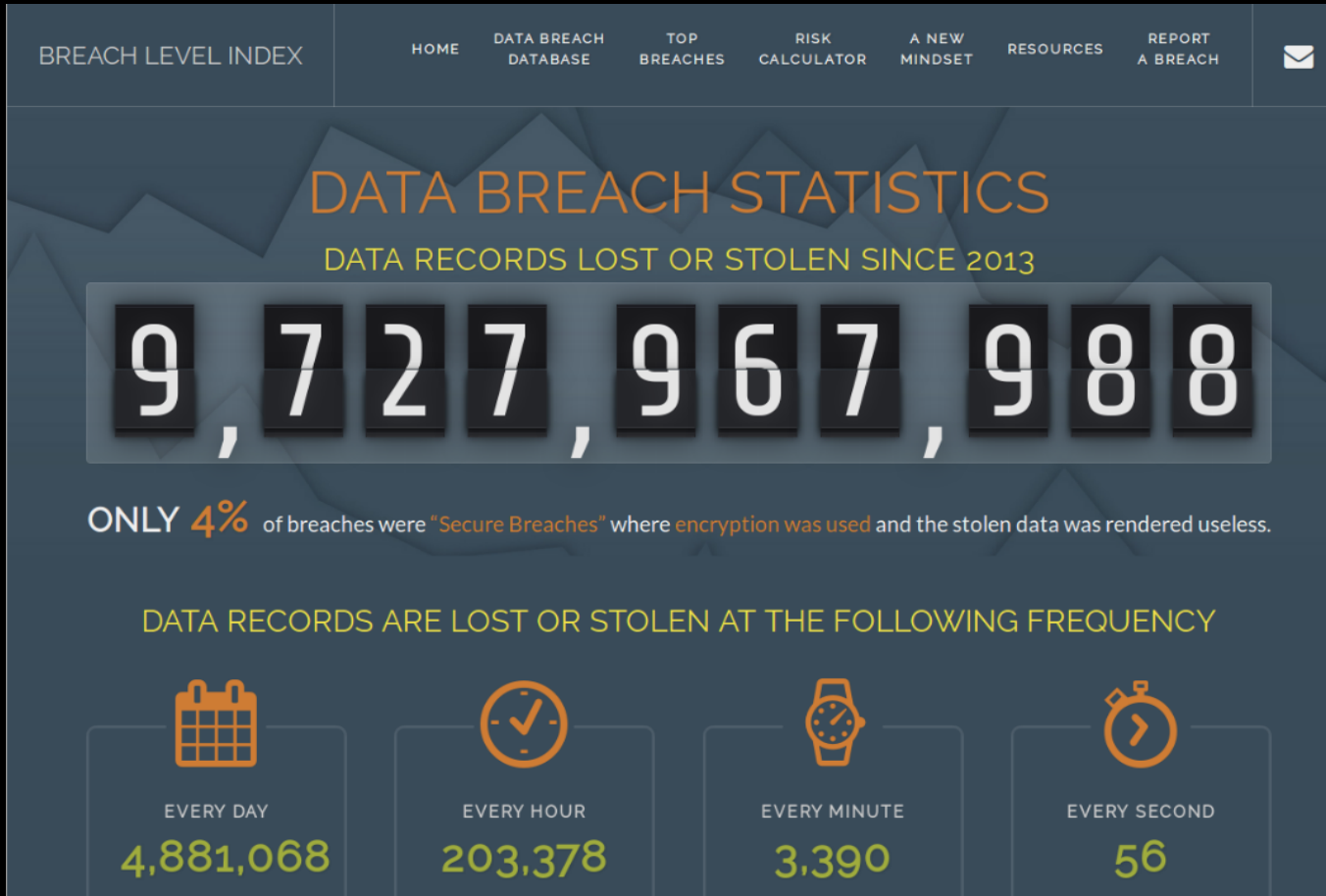


# How do we learn and train



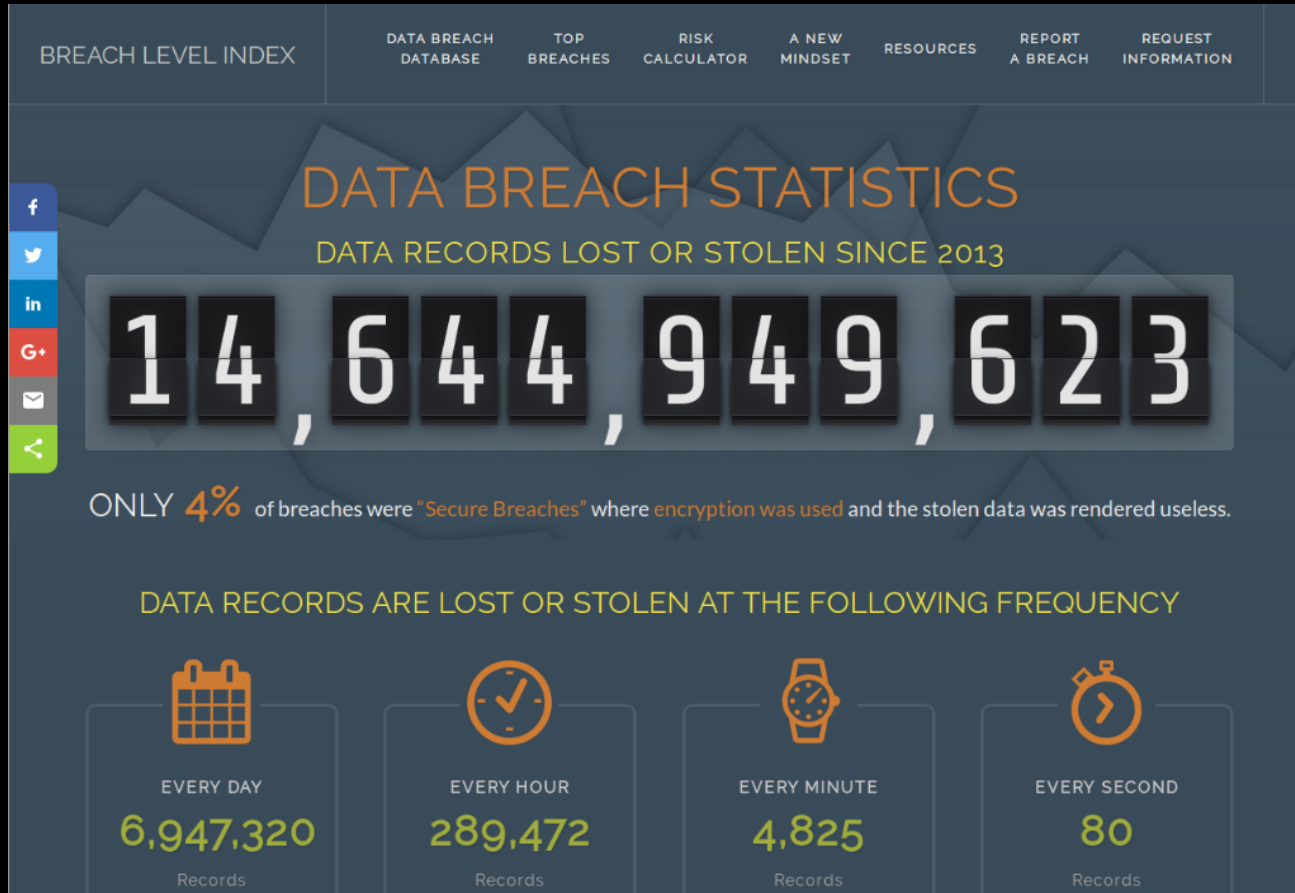


# BreachLevelIndex.com

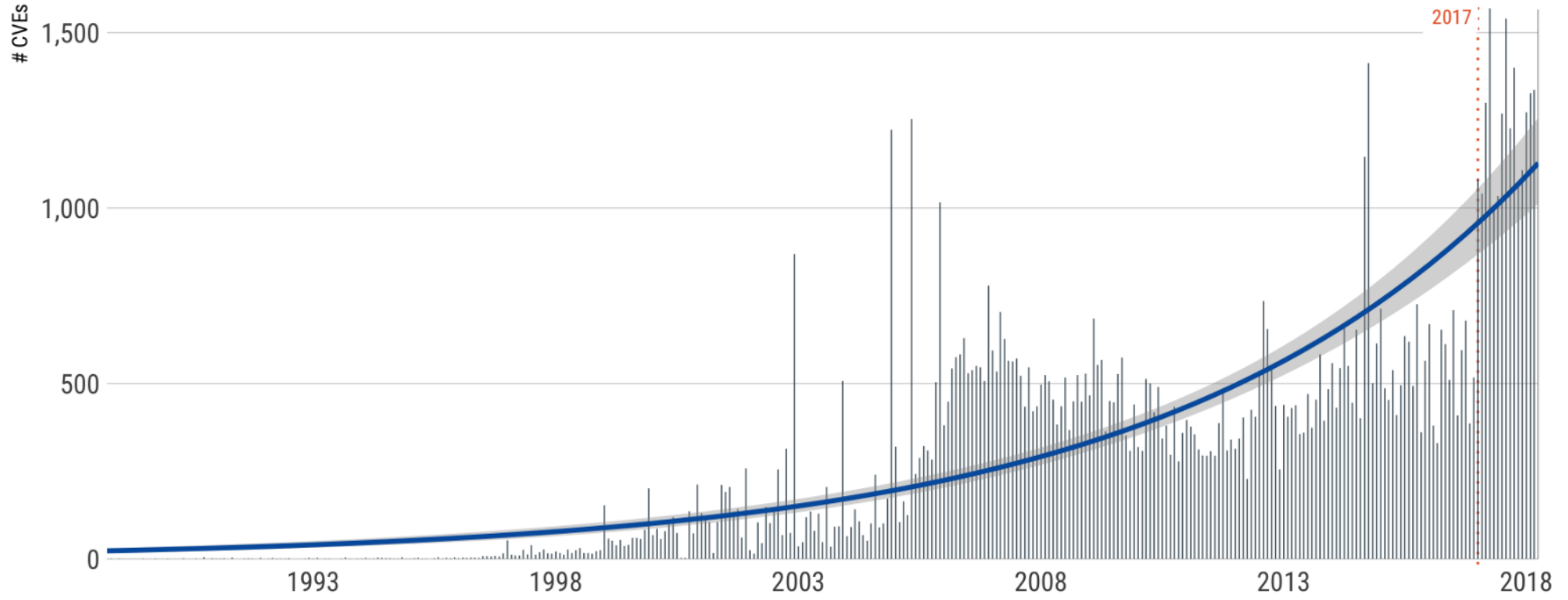




# BreachLevelIndex.com



# # CVE's per year/month



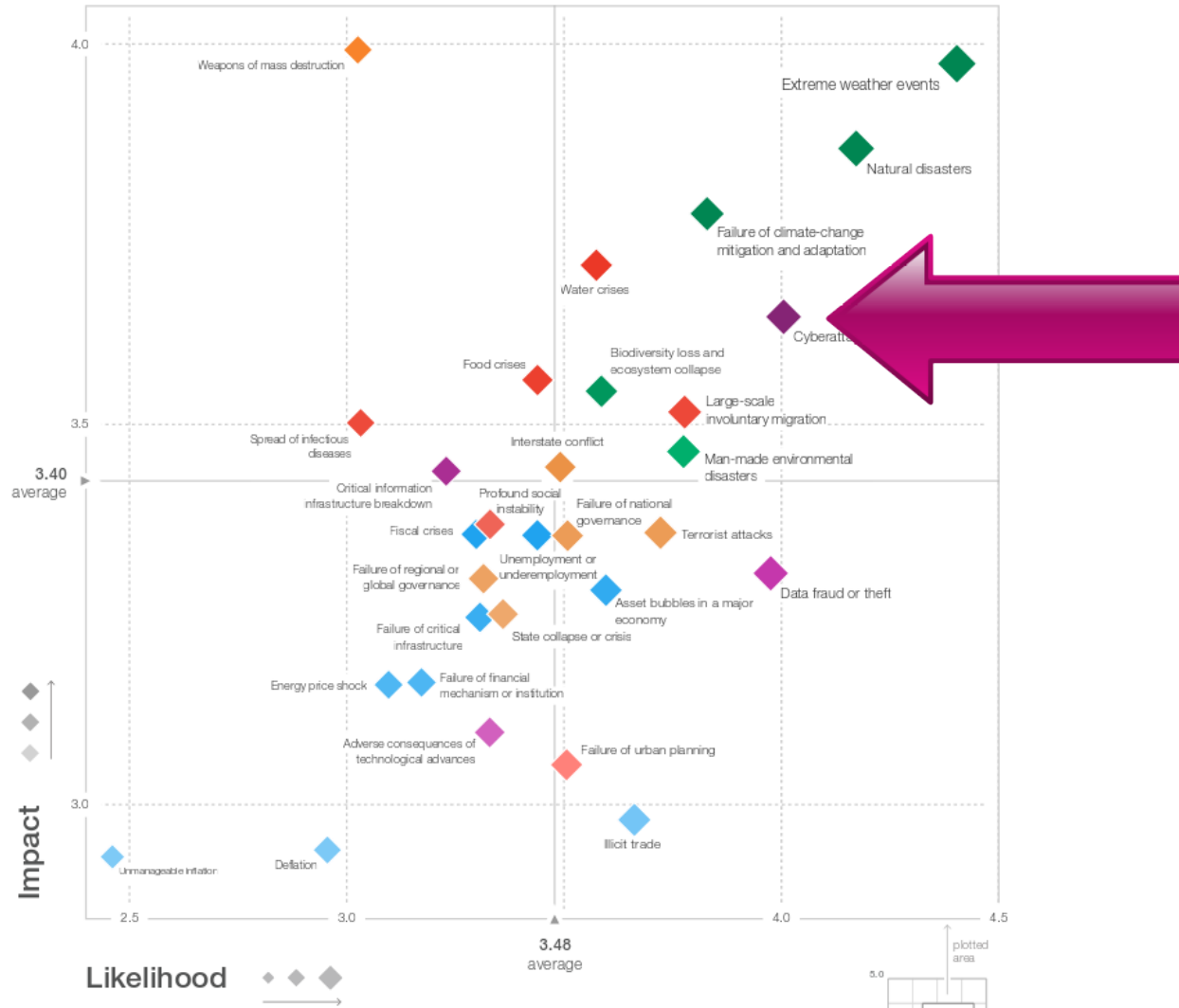
Data compiled from MITRE, NVD and Rapid7

Insight Report

# The Global Risks Report 2018 13th Edition



Figure I: The Global Risks Landscape 2018







# What's wrong

- Nothing wrong with golf
- ... or training for golf
- ... if you're going to play golf.



Image: Costume SuperCentre

## *The Four Levels of Cyberwar*

Grand Strategy  
(Political)

Strategy

Tactics

Operations





# TRIZ

- Russian - “Theory of Inventive Problem Solving”
- Characteristics of problems
- Patterns in solutions
- A sufficient level of abstraction
- Use other’s solutions





**01) DIVISION**  
 a) ship built, made of removable/replaceable bulkheads  
 b) multi-engine aircraft  
 c) multi-piston engine of internal combustion  
 d) a toy made from Lego blocks

b) breakable chocolate  
 1) multi-grip rotors  
 2) a bonded file of paper sheets  
 3) multi-blade cartridge razors  
 4) multi-blade aircrews of aircrafts, or wind power-plants

**02) TAKING OUT**  
 a) taking of notoriously noisy power unit, or compressor out of the main boat  
 b) (engines, turbines, blades) combined with internal ducts for air ventilation system, taken out of the building, i.e. placed on the building elevations  
 c) sound of bird's predator, previously registered on a tape, and played back, can be used scaring away the birds, notoriously flying near or around the airports

**03) LOCAL QUALITY**  
 a) dustless excavation of coal  
 b) bigger droplets outside of the cone  
 c) weighed average from marks

a) the dust is captured by tiny droplets inside of the water cone  
 b) weighed estimation produced for rewriting of computers, printers, etc.

**04) ASYMMETRY**  
 a) pneumatic tyre asymmetrically reinforced from outside, due to contact with pavement curb  
 b) left- or right-handed rules of priority  
 c) slanted concrete mixer, blender  
 d) asymmetrically built car, due to either left- or right-sided driver's sit

a) asymmetrically defined functionality of the "trap-the-door" mechanisms  
 f) asymmetrically built car, due to either left- or right-sided driver's sit

**05) MERGING**  
 a) several computers combined into functioning network  
 b) a hedge made of pales  
 c) roofing tiles combined into coverage of house roof  
 d) mobile concrete mixer, mobile crane, refrigerator, merged into single mobile machine unit, combining of the stationary machines with mobile undercarriages

**06) UNIVERSALITY**  
 a) a helmet in use, rendered as:  
 1) spade  
 2) frying pane  
 3) Swiss Army knife  
 b) universal within field conditions, "handy-tools"  
 c) sets of universal kitchen robots, mixers, blenders, with operating actuators (rasps, juice extractors, etc.)

**07) EMBEDDED STRUCTURES (nested "Dolls" - Matryoshka)**  
 a) radiators of ultrasound welders

**08) ANTI-WEIGHT (balance preserving)**  
 a) wind turbines (inverted) of vertical axis  
 b) semi-aircrew  
 c) fish bladder (fish submerged in water)  
 d) balloon filled with hot air  
 e) slipping hydrofoils boats  
 f) concept of hover crafts

a) wind turbines (inverted) of vertical axis  
 b) semi-aircrew  
 c) fish bladder (fish submerged in water)  
 d) balloon filled with hot air  
 e) slipping hydrofoils boats  
 f) concept of hover crafts

**09) PRE-ELIMINARY ANTI-ACTION (COUNTER- ACTION)**  
 a) basically, as well as particularly:  
 1) surrounding sounds  
 2) counter-acting active sounds  
 3) piezoelectric anti-impact system for cutting tool

a) basically, as well as particularly:  
 1) surrounding sounds  
 2) counter-acting active sounds  
 3) piezoelectric anti-impact system for cutting tool

**10) PRE-ELIMINARY ACTION**  
 a) for instance, a method of "dressing" of the cut tree branches (this action, actually forces a tree to beforehand reaction, to gather healing substances)  
 b) driver's airbag  
 c) masking of the chosen elements, with patches on the object, before its painting

a) for instance, a method of "dressing" of the cut tree branches (this action, actually forces a tree to beforehand reaction, to gather healing substances)  
 b) driver's airbag  
 c) masking of the chosen elements, with patches on the object, before its painting

**11) BEFOREHAND CUSHIONING**  
 a) piezoelectric engine - a conceptual design  
 b) spring based lighters for set of two discs  
 c) quartz generators, in electric circuits

a) piezoelectric engine - a conceptual design  
 b) spring based lighters for set of two discs  
 c) quartz generators, in electric circuits

**12) EQUIPOTENTIALITY**  
 a) a sequence of linear movements is replaced by single seamless movement on section of arc  
 b) dissolvable surgeon threads  
 c) rather to cool down stuck inner object, than to heat up against bigger outer object, which seizes the former one

a) a sequence of linear movements is replaced by single seamless movement on section of arc  
 b) dissolvable surgeon threads  
 c) rather to cool down stuck inner object, than to heat up against bigger outer object, which seizes the former one

**13) INVERSION (UPSIDE DOWN)**  
 a) for instance:  
 1) reversing the working mode of vacuum cleaner (then, vapour could be used in cleaning of carpets)  
 2) turn mounted object upside down, on assembling line  
 b) turning (object in move, while motorless turning tool, against milling (metallic milling cutter)  
 c) binary tree's structure is sought from root to leaves in one (in-depth) search algorithms, while another algorithm seeks through nodes from leaves to root

a) for instance:  
 1) reversing the working mode of vacuum cleaner (then, vapour could be used in cleaning of carpets)  
 2) turn mounted object upside down, on assembling line  
 b) turning (object in move, while motorless turning tool, against milling (metallic milling cutter)  
 c) binary tree's structure is sought from root to leaves in one (in-depth) search algorithms, while another algorithm seeks through nodes from leaves to root

**14) SPHEROIDALITY, CURVATURES**  
 a) applications of:  
 1) bearing rollers, spirals, semi-domes  
 2) application of arcs in architecture  
 3) circular accelerators (synchrotrons) in place of concept of linear accelerators of particles  
 4) extensible, retractable measuring tape

a) applications of:  
 1) bearing rollers, spirals, semi-domes  
 2) application of arcs in architecture  
 3) circular accelerators (synchrotrons) in place of concept of linear accelerators of particles  
 4) extensible, retractable measuring tape

**15) DYNAMICS**  
 a) automatically extensible/opened doors, air-locks, etc., reacting when it is needed  
 b) automatic gears in robotics  
 c) undercarriages in cars of variable stiffness characteristics, tuned exactly to terrain conditions during the driving  
 d) electronic controllers for carburettor, electronically controlled fuel injection in dependency of driving conditions

a) automatically extensible/opened doors, air-locks, etc., reacting when it is needed  
 b) automatic gears in robotics  
 c) undercarriages in cars of variable stiffness characteristics, tuned exactly to terrain conditions during the driving  
 d) electronic controllers for carburettor, electronically controlled fuel injection in dependency of driving conditions

**16) EXCESSIVE (OR PARTIAL) ACTION**  
 a) in close fit between both piston and cylinder of the engine  
 b) to spray excessively paint, and then to remove the excess of the paint  
 c) to fulfil the fuel tank, and then to remove the excess of fuel

a) in close fit between both piston and cylinder of the engine  
 b) to spray excessively paint, and then to remove the excess of the paint  
 c) to fulfil the fuel tank, and then to remove the excess of fuel

**17) ANOTHER DIMENSION**  
 a) two soldering tools in 1D should be rearranged in 2D space  
 b) to stack vertically containers, chairs, laptops, etc.  
 c) division of complex symmetries in crystallography

a) two soldering tools in 1D should be rearranged in 2D space  
 b) to stack vertically containers, chairs, laptops, etc.  
 c) division of complex symmetries in crystallography

**18) MECHANICAL SELF-INDUCED VIBRATIONS (IN RESONANCE)**  
 a) piezoelectric engine - a conceptual design  
 b) spring based lighters for set of two discs  
 c) quartz generators, in electric circuits

a) piezoelectric engine - a conceptual design  
 b) spring based lighters for set of two discs  
 c) quartz generators, in electric circuits

**19) PERIODICAL ACTION, OR PULSED ACTION**  
 a) hammer  
 b) pulsed laser, against laser  
 c) pulsed laser, against laser  
 d) pulse DC power unit  
 e) step motors

a) hammer  
 b) pulsed laser, against laser  
 c) pulsed laser, against laser  
 d) pulse DC power unit  
 e) step motors

**20) CONTINUITY ACTION OF USEFUL ACTION**  
 a) alternating drill, operating in both directions  
 b) turning of generators for one power plants, working continuously (optimal mode), while the others working, as pump-storage power plants, in aim of storing of energy for afternoon hours (under pumping of the water into reservoir on mornings, while emptying upper reservoir into lower one on afternoons)

a) alternating drill, operating in both directions  
 b) turning of generators for one power plants, working continuously (optimal mode), while the others working, as pump-storage power plants, in aim of storing of energy for afternoon hours (under pumping of the water into reservoir on mornings, while emptying upper reservoir into lower one on afternoons)

**21) SKIPPING, QUICK MODE, OR PACE OF REALIZATION**  
 a) wood-borne materials in quick thermal processing with preserving properties of the materials  
 b) laser treatments of blood tissue  
 c) an processing of hardy processing materials (both extremely hard and extremely brittle)  
 d) two-second pulsed lasers (two-second lasers) (various materials virtually have been engraved, while laser micro-second-second pulses)

a) wood-borne materials in quick thermal processing with preserving properties of the materials  
 b) laser treatments of blood tissue  
 c) an processing of hardy processing materials (both extremely hard and extremely brittle)  
 d) two-second pulsed lasers (two-second lasers) (various materials virtually have been engraved, while laser micro-second-second pulses)

**22) "BLESSING IN DISGUISE" (CONVERT HARM INTO BENEFIT)**  
 a) burning out, main in outskirts (to blow out) of the main fire  
 b) permafrost materials are to be "treated" with liquid nitrogen  
 c) the material's permafrost rapidly "liquefies"

a) burning out, main in outskirts (to blow out) of the main fire  
 b) permafrost materials are to be "treated" with liquid nitrogen  
 c) the material's permafrost rapidly "liquefies"

**23) FEEDBACK PRINCIPLE**  
 a) input signal  
 b) autopilot provided with 3-axis gyro system  
 c) robot arms movement's back-controlled in set of:  
 1) discs - 2) photo-discs - 3) semi-transparent ether: protractor, or linear scale - placed in between

a) input signal  
 b) autopilot provided with 3-axis gyro system  
 c) robot arms movement's back-controlled in set of:  
 1) discs - 2) photo-discs - 3) semi-transparent ether: protractor, or linear scale - placed in between

**24) INTERMEDIATE MEANS, "FITTING" PRINCIPLE**  
 a) in electronic circuits  
 b) fitting in mean of:  
 1) pressure-flowing (fluid mechanics),  
 2) loading of force moments,  
 3) complex transmission gears (mechanical fitting),  
 4) stress of two interfacing surfaces (endurance)

a) in electronic circuits  
 b) fitting in mean of:  
 1) pressure-flowing (fluid mechanics),  
 2) loading of force moments,  
 3) complex transmission gears (mechanical fitting),  
 4) stress of two interfacing surfaces (endurance)

**25) SELF-SERVICING PRINCIPLE**  
 a) self-servicing lamp  
 b) constant regeneration of the glow of halogen lamp  
 c) tungsten atomizes to halogens then to redepot on tungsten shaver

a) self-servicing lamp  
 b) constant regeneration of the glow of halogen lamp  
 c) tungsten atomizes to halogens then to redepot on tungsten shaver

**26) COPYING, IMAGING PRINCIPLE (application of optical mapping)**  
 a) use of ultrasonics  
 b) magnetic resonance  
 c) X-rays radiography  
 d) main mapping of material structures  
 e) use of fluorescence and scintillation's materials

a) use of ultrasonics  
 b) magnetic resonance  
 c) X-rays radiography  
 d) main mapping of material structures  
 e) use of fluorescence and scintillation's materials

**27) INEXPENSIVE SHORT-LIVED OBJECTS (CHEAP CADUCITY, & OF DISPOSABLE MATERIALS)**  
 a) kitchen utensils, dishes, cutlery made of plastic  
 b) plastic bags, packaging wrappers, etc.  
 c) printing head integrated with ink cartridge (formerly, each printer possesses built-in printing head) (presently, each ink cartridge has its own printing head)

a) kitchen utensils, dishes, cutlery made of plastic  
 b) plastic bags, packaging wrappers, etc.  
 c) printing head integrated with ink cartridge (formerly, each printer possesses built-in printing head) (presently, each ink cartridge has its own printing head)

**28A) PRINCIPLE OF SUBSTITUTING OF MECHANICAL SYSTEM WITH FUNCTIONALLY EQUIVALENT ELECTRO-MAGNETIC SYSTEMS**  
 a) electric field  
 b) magnetic field  
 c) mechanical pressure  
 d) fastening

a) electric field  
 b) magnetic field  
 c) mechanical pressure  
 d) fastening

**28B) SUBSTITUTING OF MECH. SYS. WITH ELECTRO-MAGN. SYSTEMS**  
 A) magnetic borne pressure of the machined materials  
 B) magnetic borne pressure of the machined materials  
 C) magnetic fields instead of static fields  
 D) heterogeneous fields

A) magnetic borne pressure of the machined materials  
 B) magnetic borne pressure of the machined materials  
 C) magnetic fields instead of static fields  
 D) heterogeneous fields

**29A) PNEUMATICS & HYDRAULICS**  
 a) pneumatic automobile tyre, pneumatic (air-light) dampers, automobile airbrags, pneumatic "disc-brake", diving of operational actuators, for instance, in automatic welding of packaging covers made of plastic wrapping  
 b) on the figure above, in blue: approximate section of automobile pneumatic tyre

a) pneumatic automobile tyre, pneumatic (air-light) dampers, automobile airbrags, pneumatic "disc-brake", diving of operational actuators, for instance, in automatic welding of packaging covers made of plastic wrapping  
 b) on the figure above, in blue: approximate section of automobile pneumatic tyre

**29B) PNEUMATICS & HYDRAULICS**  
 a) automobile brakes, in driving of plane elevator, where the precision of driving is needed, as well as enormous force transition  
 b) hydraulics in communicating vessels  
 c) pressure-flowing (fluid mechanics), loading of force moments, complex transmission gears (mechanical fitting), stress of two interfacing surfaces (endurance)

a) automobile brakes, in driving of plane elevator, where the precision of driving is needed, as well as enormous force transition  
 b) hydraulics in communicating vessels  
 c) pressure-flowing (fluid mechanics), loading of force moments, complex transmission gears (mechanical fitting), stress of two interfacing surfaces (endurance)

**30) FLEXIBLE FILMS, FOILS, MEMBRANES**  
 a) not available film protection of water  
 b) wrapping packaging based on plastic, air-pumped bubbles  
 c) foldable balloons, domes, barriers

a) not available film protection of water  
 b) wrapping packaging based on plastic, air-pumped bubbles  
 c) foldable balloons, domes, barriers

**31) POROUS MATERIALS**  
 a) aerated concrete (pore concrete)  
 b) porous abrasive tools  
 c) polyurethane foam  
 d) catalyzing surfaces in chemistry  
 e) "vacuum" mapping as a "construction building material"  
 f) openwork structures reinforcements

a) aerated concrete (pore concrete)  
 b) porous abrasive tools  
 c) polyurethane foam  
 d) catalyzing surfaces in chemistry  
 e) "vacuum" mapping as a "construction building material"  
 f) openwork structures reinforcements

**32) COLOUR CHANGING (ALTERNATING)**  
 a) in lapping process for inner surfaces of engine pistons & cylinders, the probing of phosphorescence distribution can be used

a) in lapping process for inner surfaces of engine pistons & cylinders, the probing of phosphorescence distribution can be used

**33) HOMOGENEITY**  
 a) the two interfacing surfaces should be made of the same material  
 b) moreover, the similarities can be applied, regarding:  
 1) comparable that hardness, chemical inertion, structures,  
 2) comparable thermal expansion's coefficients, (in case of dental materials; metal-glass conjunctions),  
 3) comparable electro-chemical potentials, (in avoiding electro-chemical borne corrosion)  
 4) same fatigue characteristics, and amortization specifics

a) the two interfacing surfaces should be made of the same material  
 b) moreover, the similarities can be applied, regarding:  
 1) comparable that hardness, chemical inertion, structures,  
 2) comparable thermal expansion's coefficients, (in case of dental materials; metal-glass conjunctions),  
 3) comparable electro-chemical potentials, (in avoiding electro-chemical borne corrosion)  
 4) same fatigue characteristics, and amortization specifics

**34) DISCARDING & RECOVERING, (REJECT & PARTS REGENERATION)**  
 a) dissolvable medication capsules made of (biologically inert material) during the flight  
 b) rocket's stages subsequently discarded during the flight  
 c) cornstarch packages for dry products

a) dissolvable medication capsules made of (biologically inert material) during the flight  
 b) rocket's stages subsequently discarded during the flight  
 c) cornstarch packages for dry products

**35) CHANGING STATE, PARAMETERS, PROPERTIES OF MATERIALS**  
 1) high temperature food processing  
 2) low temperature processing (for submerging in liquid chocolate)  
 3) a product ready for further processing (e.g. submerging in liquid chocolate)

1) high temperature food processing  
 2) low temperature processing (for submerging in liquid chocolate)  
 3) a product ready for further processing (e.g. submerging in liquid chocolate)

**36) PHASE TRANSITION**  
 a) binary, phase transition cycle for refrigerator construction  
 b) heat flows from surroundings (red arrows directed to blue heat exchanger) to evaporator  
 c) heat carrier, (three, ammonia, etc.) circulation of an external fluid in heat exchanger

a) binary, phase transition cycle for refrigerator construction  
 b) heat flows from surroundings (red arrows directed to blue heat exchanger) to evaporator  
 c) heat carrier, (three, ammonia, etc.) circulation of an external fluid in heat exchanger

**37) THERMAL EXPANSION**  
 1) thermal shaft fitting  
 2) state of thermal balance

1) thermal shaft fitting  
 2) state of thermal balance

**38) STRONG OXIDANTS**  
 a) oxygen in oxidation of metal's surface (great with over-heated vapour under pressure, at 300°C degree)  
 b) ozone  
 c) (indirectly vapour) H<sub>2</sub>O  
 d) with protection layer obtained due to oxidation

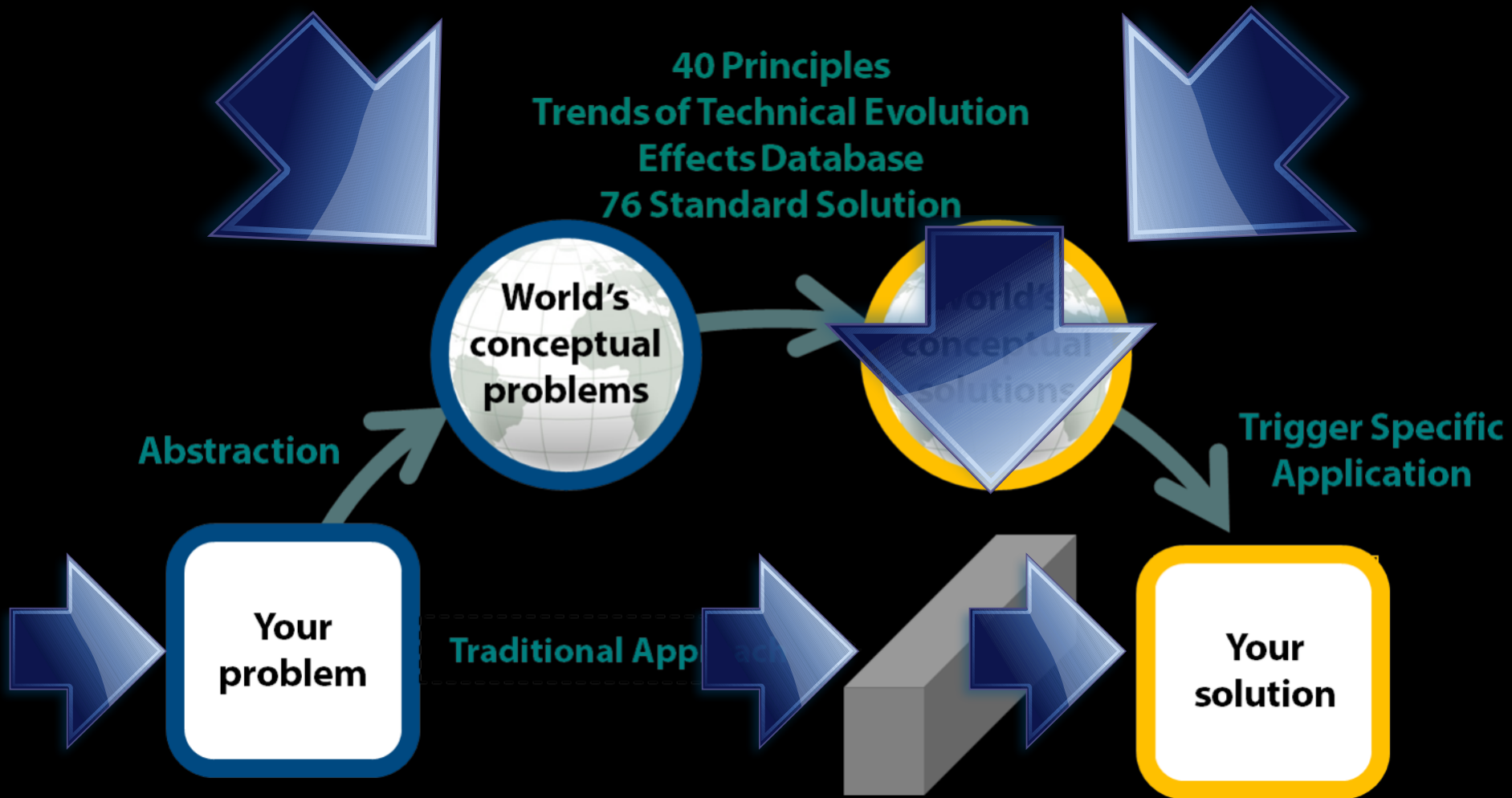
a) oxygen in oxidation of metal's surface (great with over-heated vapour under pressure, at 300°C degree)  
 b) ozone  
 c) (indirectly vapour) H<sub>2</sub>O  
 d) with protection layer obtained due to oxidation

**39) NEUTRAL ATMOSPHERES, INERT ENVIRONMENTS**  
 a) CO<sub>2</sub> extinguishers  
 b) N<sub>2</sub> or He<sub>2</sub> production atmospheres in processing, and production  
 c) N<sub>2</sub> or He<sub>2</sub> protection atmospheres in storing of products, and materials, both raw and processed

a) CO<sub>2</sub> extinguishers  
 b) N<sub>2</sub> or He<sub>2</sub> production atmospheres in processing, and production  
 c) N<sub>2</sub> or He<sub>2</sub> protection atmospheres in storing of products, and materials, both raw and processed

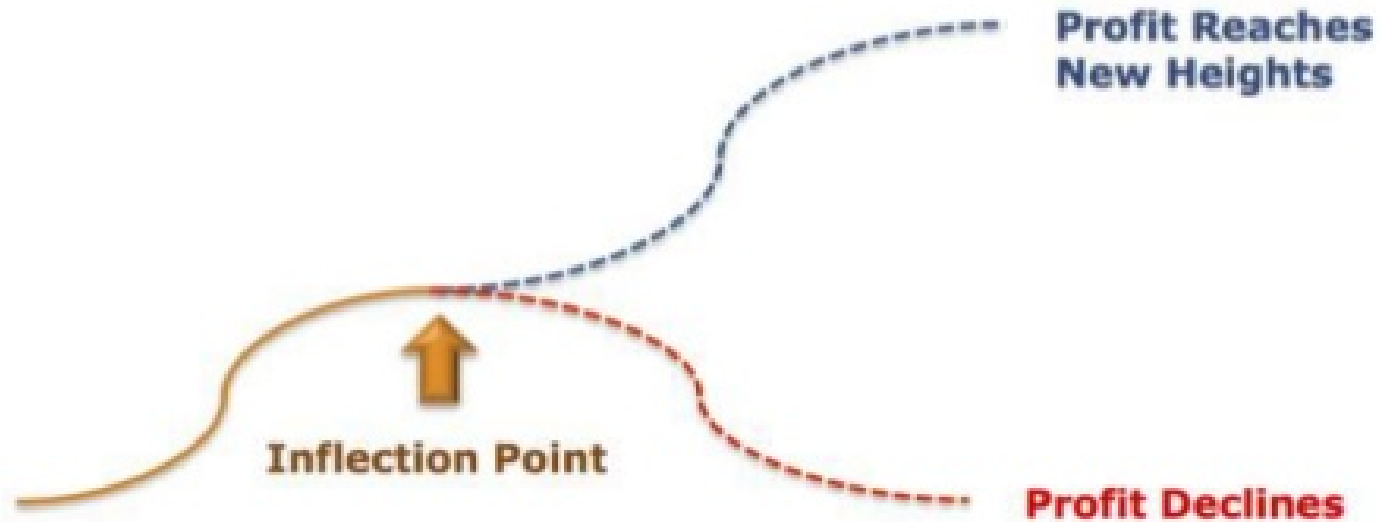
**40) COMPOSITE MATERIALS**  
 1) elements of blades, rotors, aircrews in wind turbines constructions;  
 2) yacht's & catamaran's constructions;  
 3) elements exposed to ultra-strong, severe stress

1) elements of blades, rotors, aircrews in wind turbines constructions;  
 2) yacht's & catamaran's constructions;  
 3) elements exposed to ultra-strong, severe stress

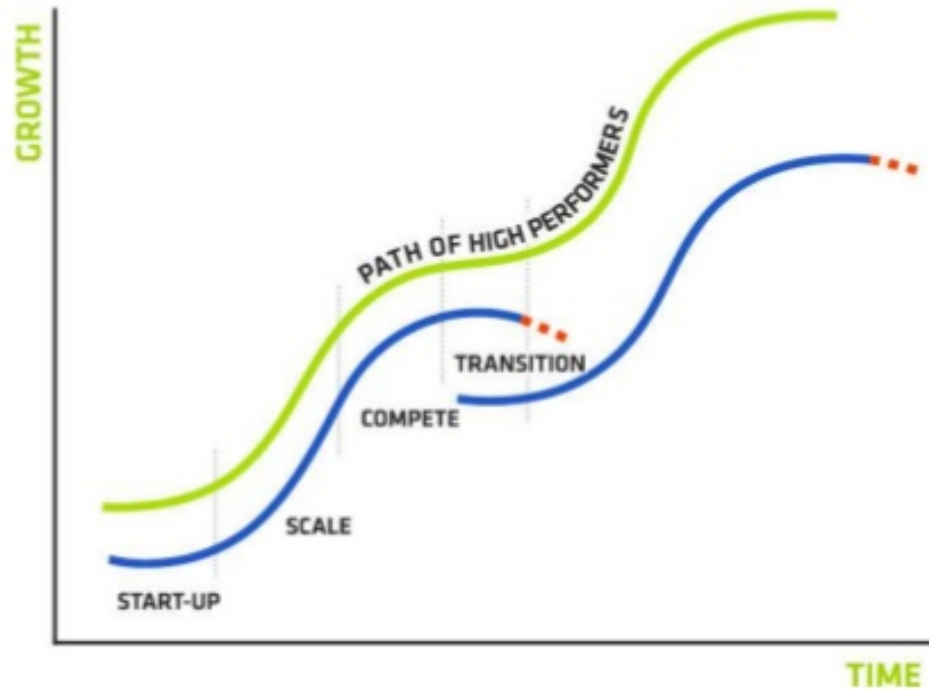




# Strategic Inflection Point



# Double S-Curve Model



2013 LIFT Conference: Driving Innovation-Based Growth



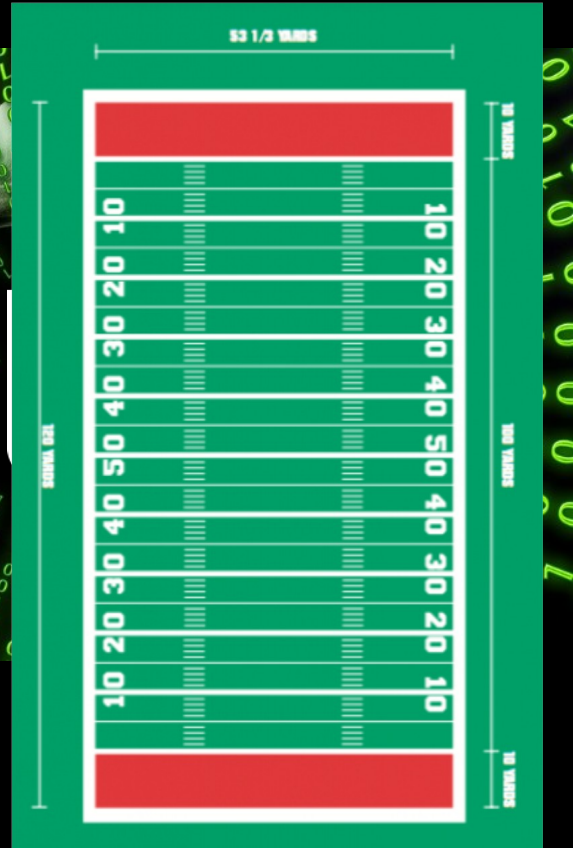
So ...



42

A person wearing a red jersey with the number 42 in white. They are holding a baseball glove in their left hand. The background is dark, possibly a locker room, with some light fixtures visible.

- Utterly incomprehensible from outside
- Complex
- Team games
- Highly specialised
  - By situation
  - Attack or Defend
- Fight over territory
- Offensive or defensive playbooks

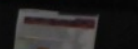
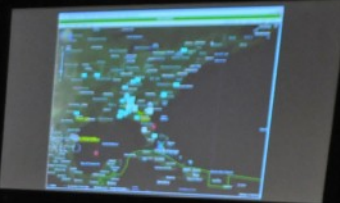
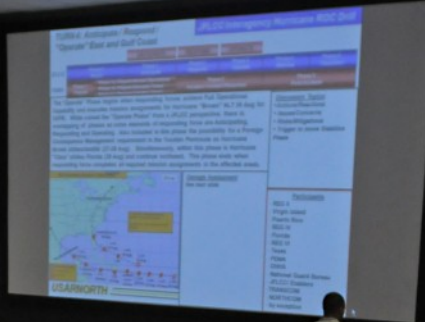






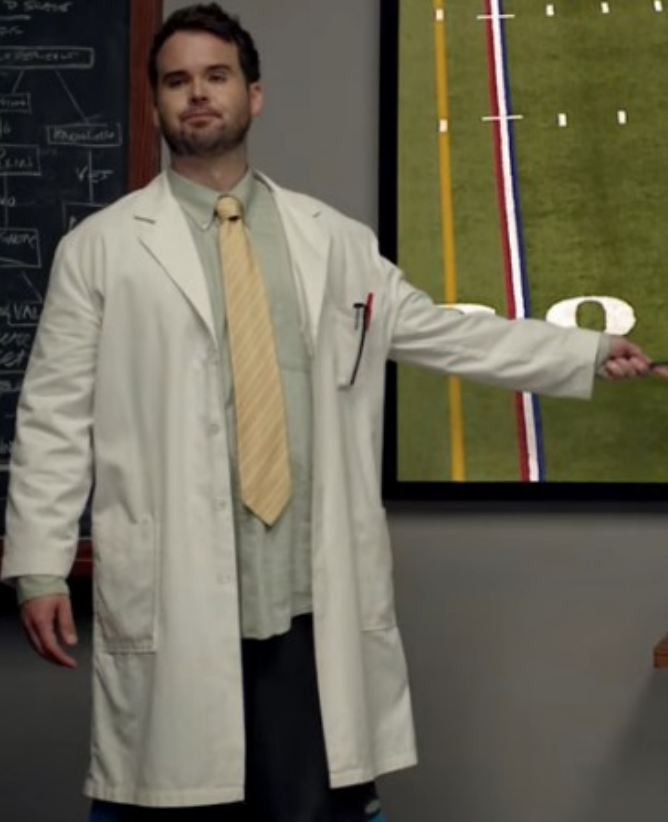
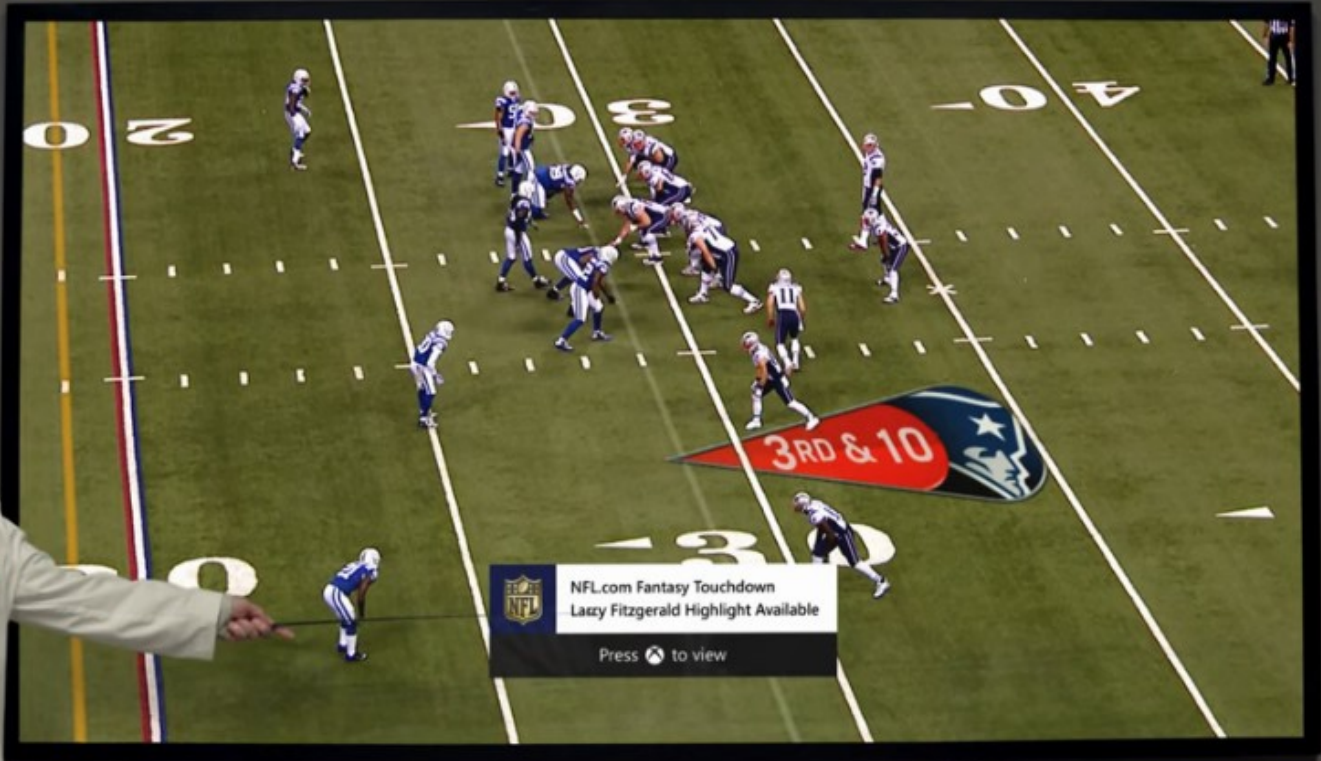
<https://media.defense.gov/>

Nick Drage – Path Dependence – @SonOfSunTzu



Region  
Overview





Screens simulated; subject to change.





# SEATTLE SEAHAWKS



Offense	Starter	2nd String	3rd String
QB	Russell Wilson	<b>Tarvaris Jackson</b>	Terrelle Pryor
HB	Marshawn Lynch	Robert Turbin	
HB2	Christine Michael		
FB	Derrick Coleman	Spencer Ware	Kiero Small
TE-Y	Zach Miller	<b>Anthony McCoy</b>	
TE-H	Luke Willson		
WR1	Percy Harvin	Paul Richardson	Bryan Waters
WR2	Doug Baldwin	<b>Sidney Rice</b>	Ricardo Lockette
SWR	Jermaine Kearse	Kevin Norwood	
LT	Russell Okung	Alvin Bailey	
LG	James Carpenter	Caylin Hauptmann	
C	Max Unger	Lemuel Jeanpierre	Greg Van Roten
RG	J.R. Sweezy	Steve Schilling	
RT	Michael Bowie	Justin Britt	



Defense	Starter	2nd String	3rd String
DLE	Michael Bennett	Greg Scruggs	Benson Mayowa
DLT	Tony McDaniel	<b>Kevin Williams</b>	Jordan Hill/D'Anthony Smith
DRT	Brandon Mebane	Jesse Williams	Jimmy Staten
DRE	Cliff Avril	Cassius Marsh	O'Brien Schofield
SLB	Bruce Irvin	Malcolm Smith	
MLB	Bobby Wagner	<b>Heath Farwell</b>	
WLB	K.J. Wright	Michael Morgan	Kevin Pierre-Louis
LCB	Richard Sherman	Tharold Simon	AJ Jefferson
RCB	Byron Maxwell	Phillip Adams	Eric Pinkins
SCB	Jeremy Lane	DeShawn Shead	
SS	Kam Chancellor	Jeron Johnson	
FS	Earl Thomas		



Special Teams	Starter	2nd String	
K	Steven Hauschka		
P	<b>Jon Ryan</b>		
LSN	Clint Gresham		

THE LEGION OF  
**BOOM**





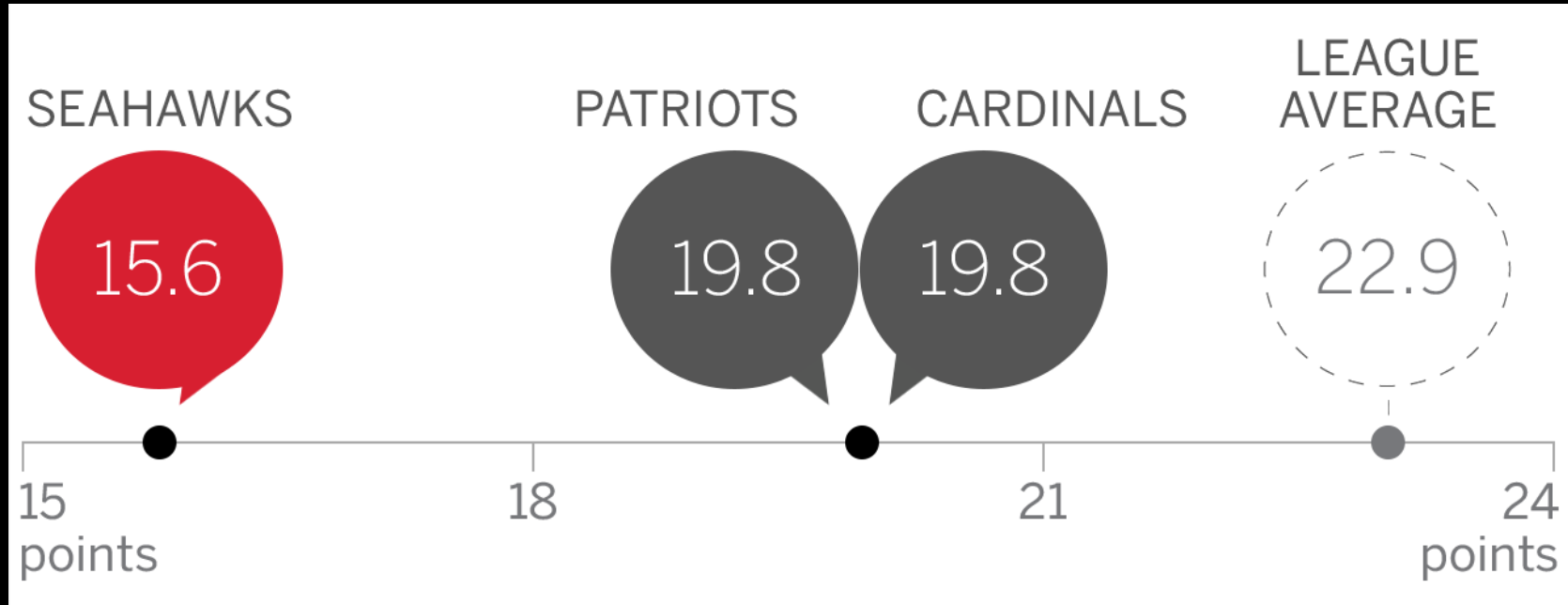
# Seattle Seahawks' Defense – 2011 to 2017

- Sherman - CornerBack
- Thomas – Free Safety
- Chancellor – Strong Safety
- Everyone



# 2012-2015

- Fewest points allowed 2012, 2013, 2014, 2015 – NFL Record



# 2012-2015

- Lead the league – Fewest Passing Yards Allowed
- Lead the league – Fewest First Downs
- 2<sup>nd</sup> Quarterback Pressures
- 4<sup>th</sup> Rushing Yards per carry
- 6<sup>th</sup> in takeaways
- Always high in DVOA ranking

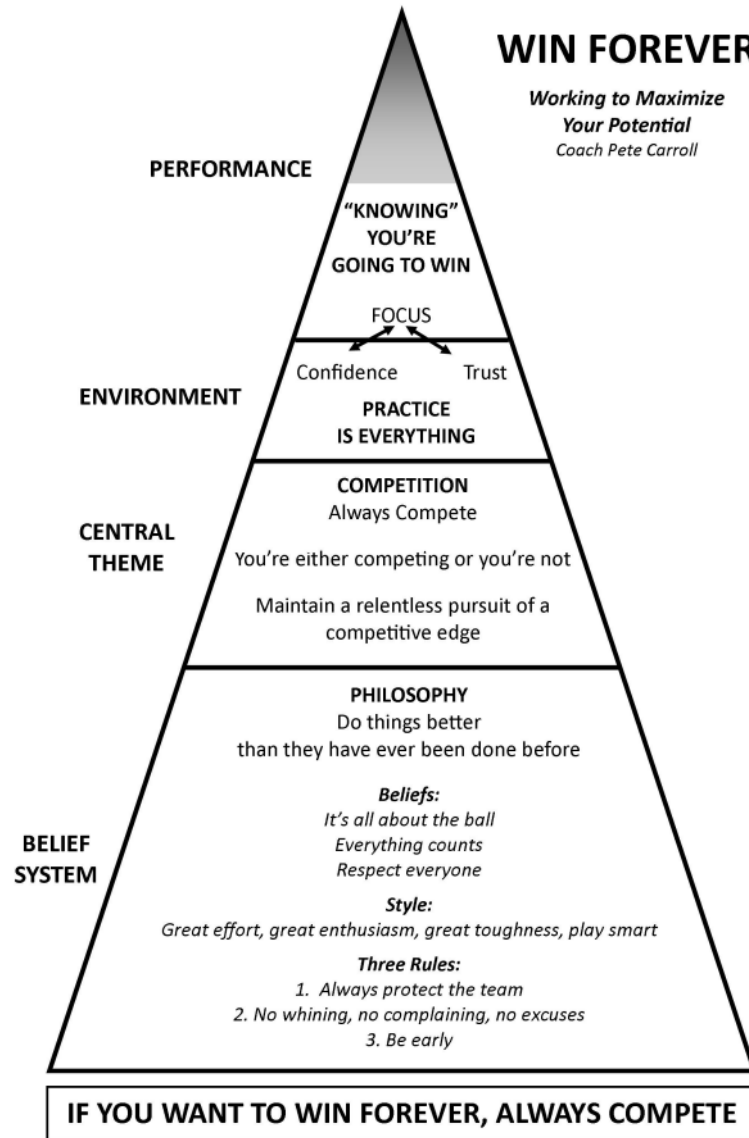


# LESSON – “shift left” your conflict





Practice is everything





# SUPER BOWL XLVIII CHAMPIONS

SUPER BOWL XLVIII

MeLife

SUPER BOWL XLVIII







# SEATTLE SEAHAWKS



Offense	Starter	2nd String	3rd String
QB	Russell Wilson	Markus Tardus	Terrelle Pryor
HB	Marshawn Lynch	Robert Turbin	
HB2	Christine Michael		
FB	Derrick Coleman	Spencer Ware	Kiero Small
TE-Y	Zach Miller	Anthony McCoy	
TE-H	Tommy Wilson		
WR1	Earl Thomas	Paul Richardson	Bryan Waters
WR2	Golden Tate	Sidney Rice	Ricardo Lockette
SWR	Earl Thomas	Kevin Norwood	
LT	Russell Hagen	Alvin Bailey	
LG	James Carpenter	Caylin Hauptmann	
C	Max Unger	Lesnel Jeanpierre	Greg Van Roten
RG	J.R. Sweezy	Steve Schilling	
RT	Michael Bowie	Justin Britt	

Defense	Starter	2nd String	3rd String
DLE	Michael Bennett	Reg Scruggs	Benson Mayowa
DLT	Tony McDermott	Kevin Williams	Jordan Hill/D'Anthony Smith
DRT	Brandon Mebane	Jesse Williams	Jimmy Staten
DRE	Clayton Kubiak	Cassius Marsh	O'Brien Schofield
SLB	Earl Thomas	Malcolm Smith	
MLB	Earl Thomas	Heath Farwell	
WLB	K.J. Wright	Michael Morgan	Kevin Pierre-Louis
LCB	Richard Sherman	Tharold Simon	AJ Jefferson
RCB	Byron Maxwell	Phillip Adams	Eric Pinkins
SCB	Jeremy Lane	DeShawn Shead	
SS	Kam Chancellor	Jeron Johnson	
FS	Earl Thomas		

Special Teams	Starter	2nd String	
K	Steven Hauschka		
P	Jon Ryan		
LSN	Clint Gresham		

# The Caffrey Triangle



## Trap #10: Threat Modeling at the Wrong Time

"Sir, we've analyzed their attack pattern, and there is a danger"





DevSecCon

# Threat Modeling at Speed & Scale

Stuart Winter-Tear

DevSecCon

The DevSecOps Conference

making continuously secure development a reality.

Image: Frasier Scott



## Breaking Ground

ATT&CKing the Status Quo: Improving Threat Intel and Cyber Defense with MITRE ATT&CK

Katie Nickels, John Wunder

### So what does this get us?

Status Quo	ATT&CKing threat intel
So. Many. Reports!	Structures threat intel so it's easier to consume a lot of it
Tough to apply intel to defenses	Provides a way to directly compare intel to defenses
Reliance on indicators	Moves to TTPs and behaviors

#### ▪ Plus!

- Gives us a common language to communicate
- Allows us to compare groups





## So what does this get us?

Status Quo	ATT&CKing threat intel
So. Many. Reports!	Structures threat intel so it's easier to consume a lot of it
Tough to apply intel to defenses	Provides a way to directly compare intel to defenses
Reliance on indicators	Moves to TTPs and behaviors

- **Plus!**

- Gives us a common language to communicate
- Allows us to compare groups

# The Base of Sand Problem

**A RAND NOTE**

**N-3148-OSD/DARPA**

**The Base of Sand Problem: A White Paper  
on the State of Military Combat Modeling**

**Paul K. Davis, Donald Blumenthal**

**Prepared for the  
Office of the Secretary of Defense  
Defense Advanced Research Projects Agency**

# Footnote 3

such as SIMNET; and knowledge-based modeling concepts. Unfortunately, however, there is a problem that has already become a limiting factor in what can be accomplished, one that is not yet widely recognized. We call this the base of sand.

---

<sup>3</sup>To illustrate how critical the use of combat models is in analyzing empirical data, consider that battle outcomes have historically borne no relationship to the raw force ratio. By contrast, when the outcome data is passed through models sensitive to situational factors such as terrain, preparations, asymmetries in fighting effectiveness due to better organization and training, and so forth, one finds that the data actually makes sense and that what matters is a ratio of *effective* forces. Unfortunately, the values of some of the key variables may not be known in advance. As a result, the models are sometimes more useful for after-the-fact description than for reliable prediction.

“Battle outcomes have historically borne no relationship to the raw force ratio...

...what matters is the ratio of effective forces” ( emphasis mine )



**Jeremiah Grossman** ✓

@jeremiahg

Follow



"Less than 2% of vulnerabilities are actively exploited in the wild, making traditional remediation very inefficient, costly, and time-consuming."



**Kenna Security** @KennaSecurity

Have you heard about our report with @cyentiainst this morning? It provides a quantitative look at the effectiveness of common remediation strategies. See the full report here: [bit.ly/2IGrlG0](https://bit.ly/2IGrlG0)

12:18 pm - 15 May 2018



# Jeremiah Grossman

CEO of Bit Discovery, Professional Hacker, Black Belt in Brazilian Jiu-Jitsu, Off-Road Race Car Driver, Founder of WhiteHat Security, and Maui resident.


MONDAY, MAY 07, 2018

## All these vulnerabilities, rarely matter.

There is a serious misalignment of interests between Application Security vulnerability assessment vendors and their customers. Vendors are incentivized to report everything they possible can, even issues that rarely matter. On the other hand, customers just want the vulnerability reports that are likely to get them hacked. Every finding beyond that is a waste of time, money, and energy, which is precisely what's happening every day. Let's begin exploring this with some context:

ABOUT ME



 [Jeremiah Grossman](#)

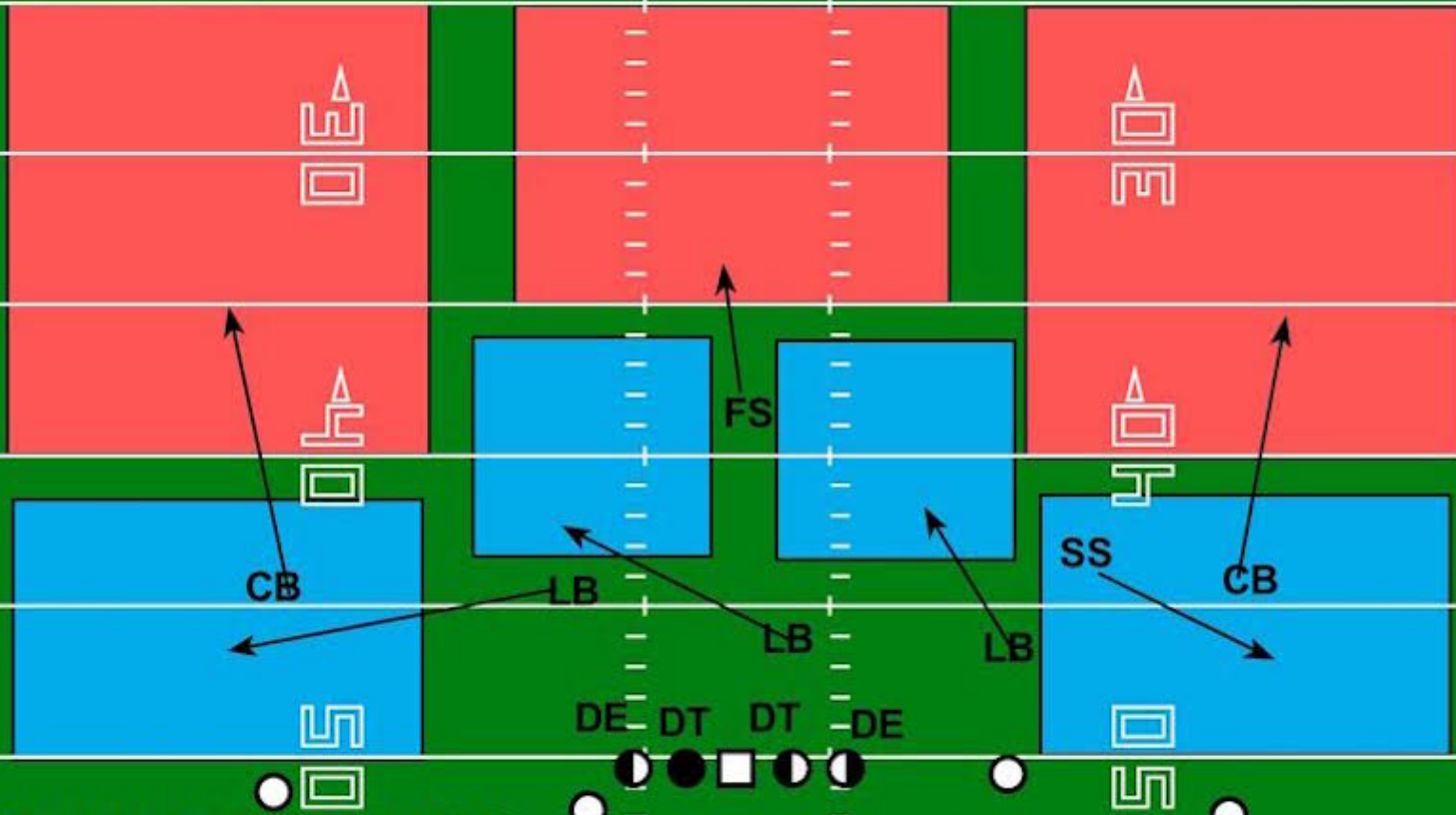
Jeremiah Grossman's career spans nearly 20 years and has lived a literal lifetime in computer security to become one of the industry's biggest

# LESSON – Eliminate the big play



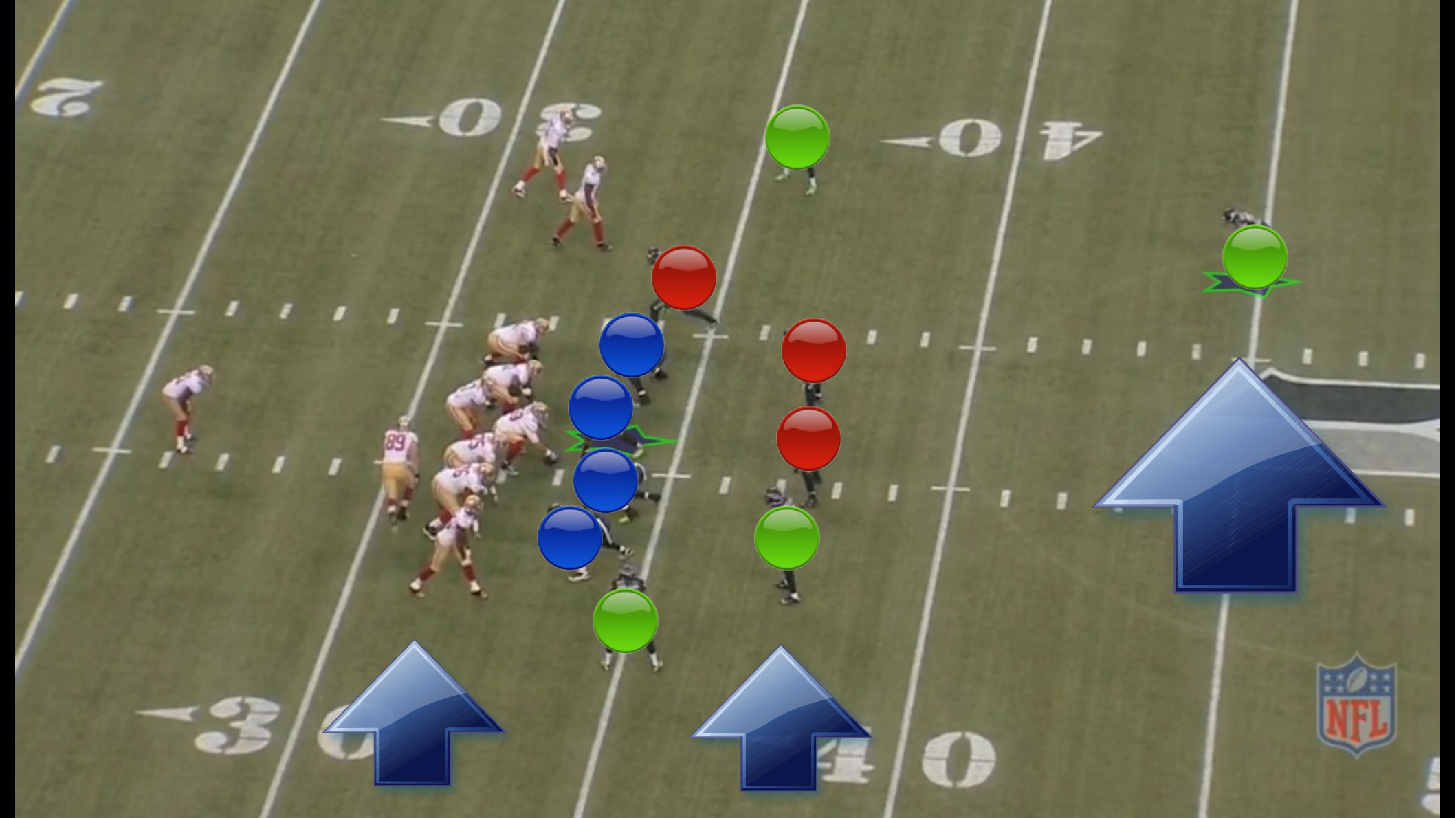
Cover 3

@ITPylon



THREE DEEP SAFETIES,  
USUALLY FS AND 2 CBs

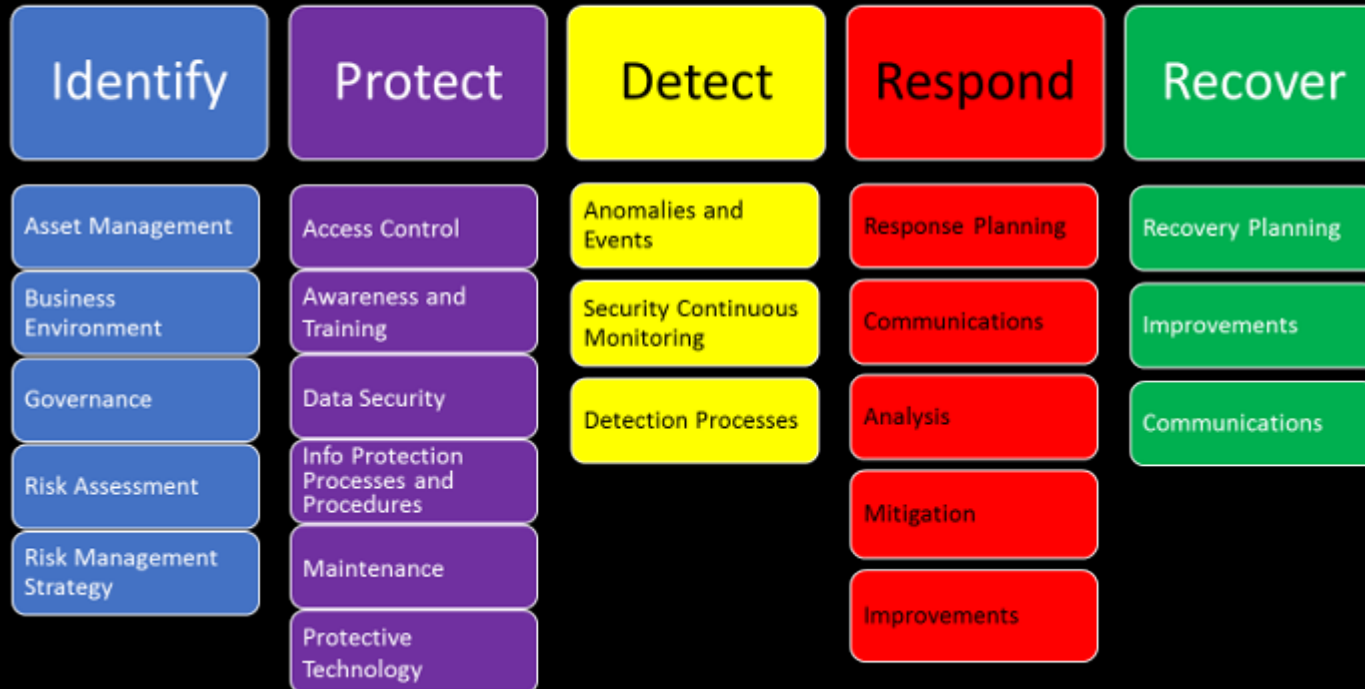
ZONE UNDERNEATH





# NIST – five core functions

## NIST Cyber Security Framework



# NIST – five core functions



# NIST – five core functions

## Security Framework

Detect

Respond

Recover

Anomalies and  
Events

Response Planning

Recovery Planning

Security Continuous  
Monitoring

Communications

Improvements

Detection Processes

Analysis

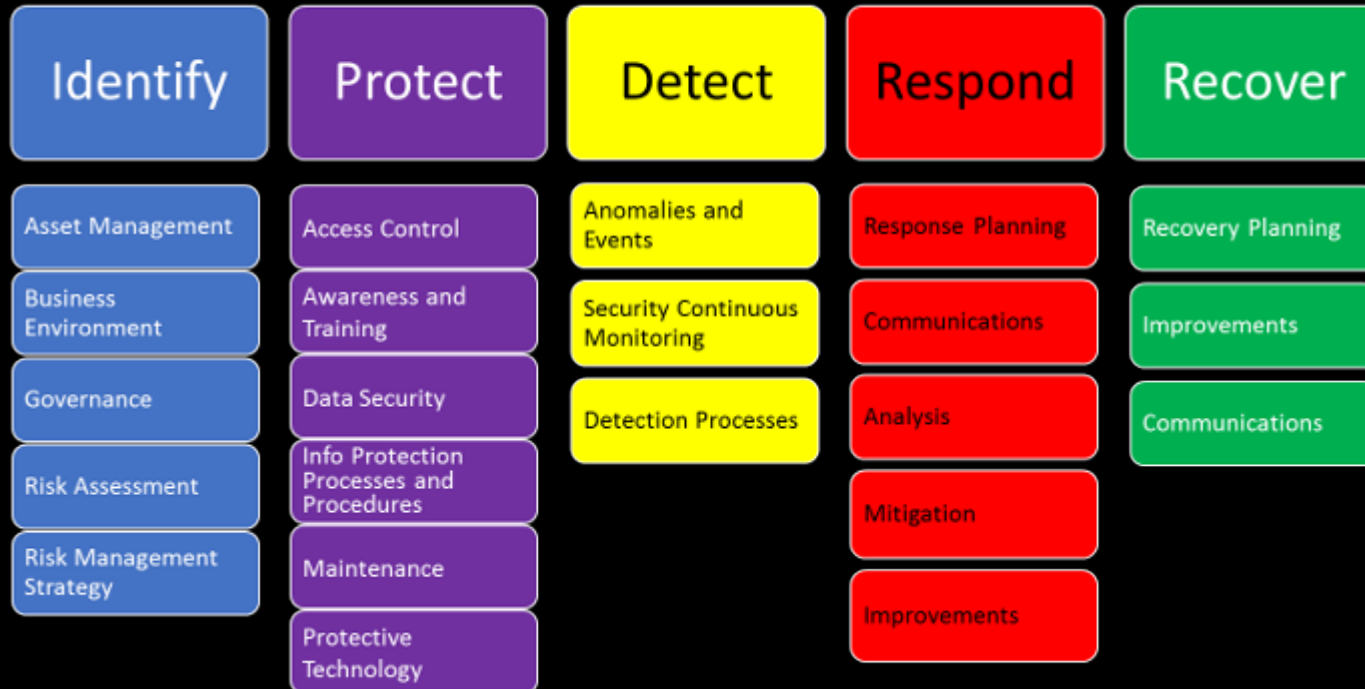
Communications

Mitigation

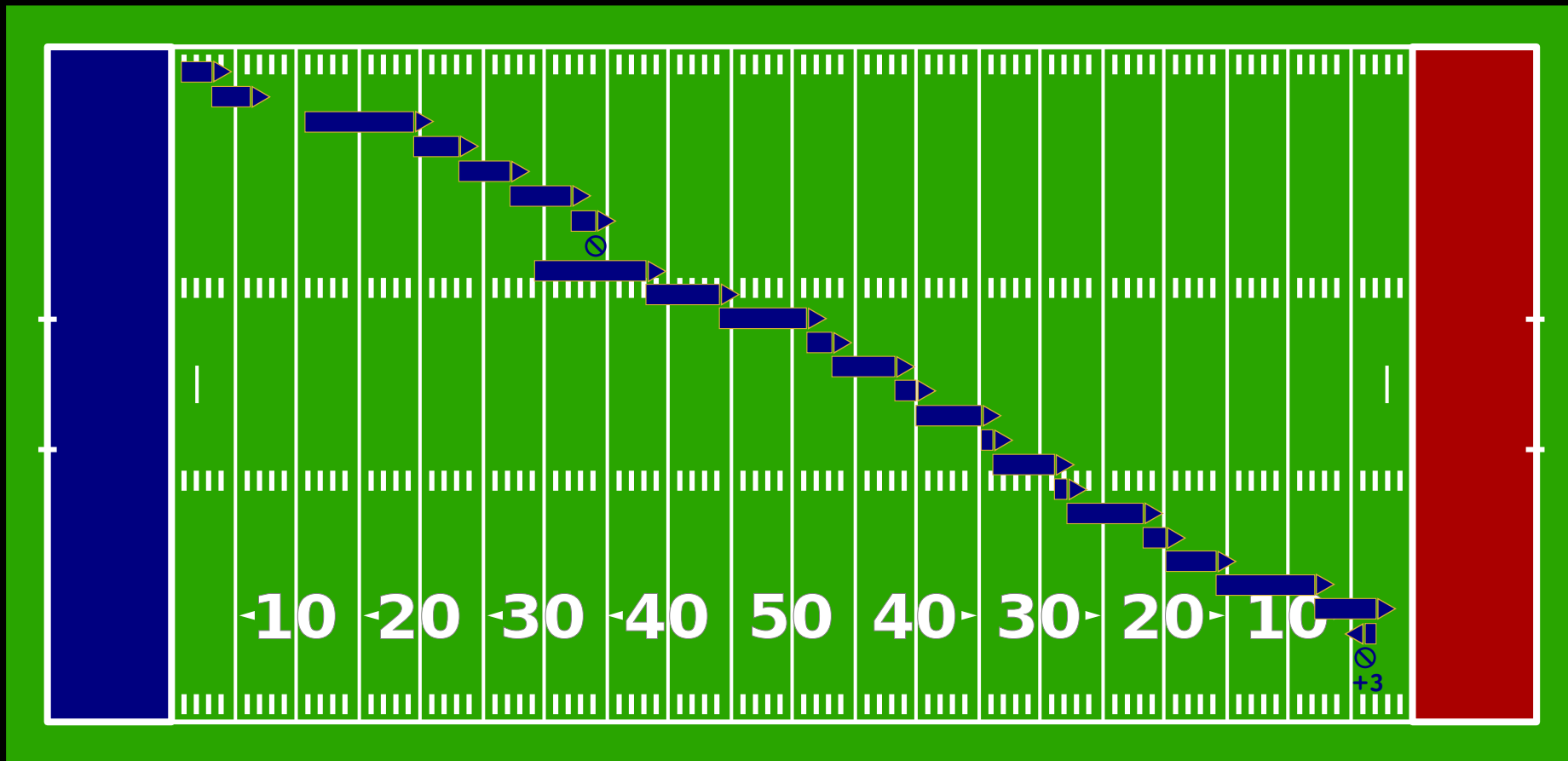
Improvements

# NIST – five core functions

## NIST Cyber Security Framework



# Drive chart





# How breaches work (perception)

## Getting hacked (common perception)

1. Attacker's Exploit Succeeds



# How breaches work (perception vs reality)



## Getting hacked (common perception)

1. Attacker's Exploit Succeeds



## Reality

1. Exploit succeeds
2. Escalate privileges
3. Scans network
4. Dumps/cracks creds
5. Pivots
6. Creates additional accounts
7. Exfiltrates data



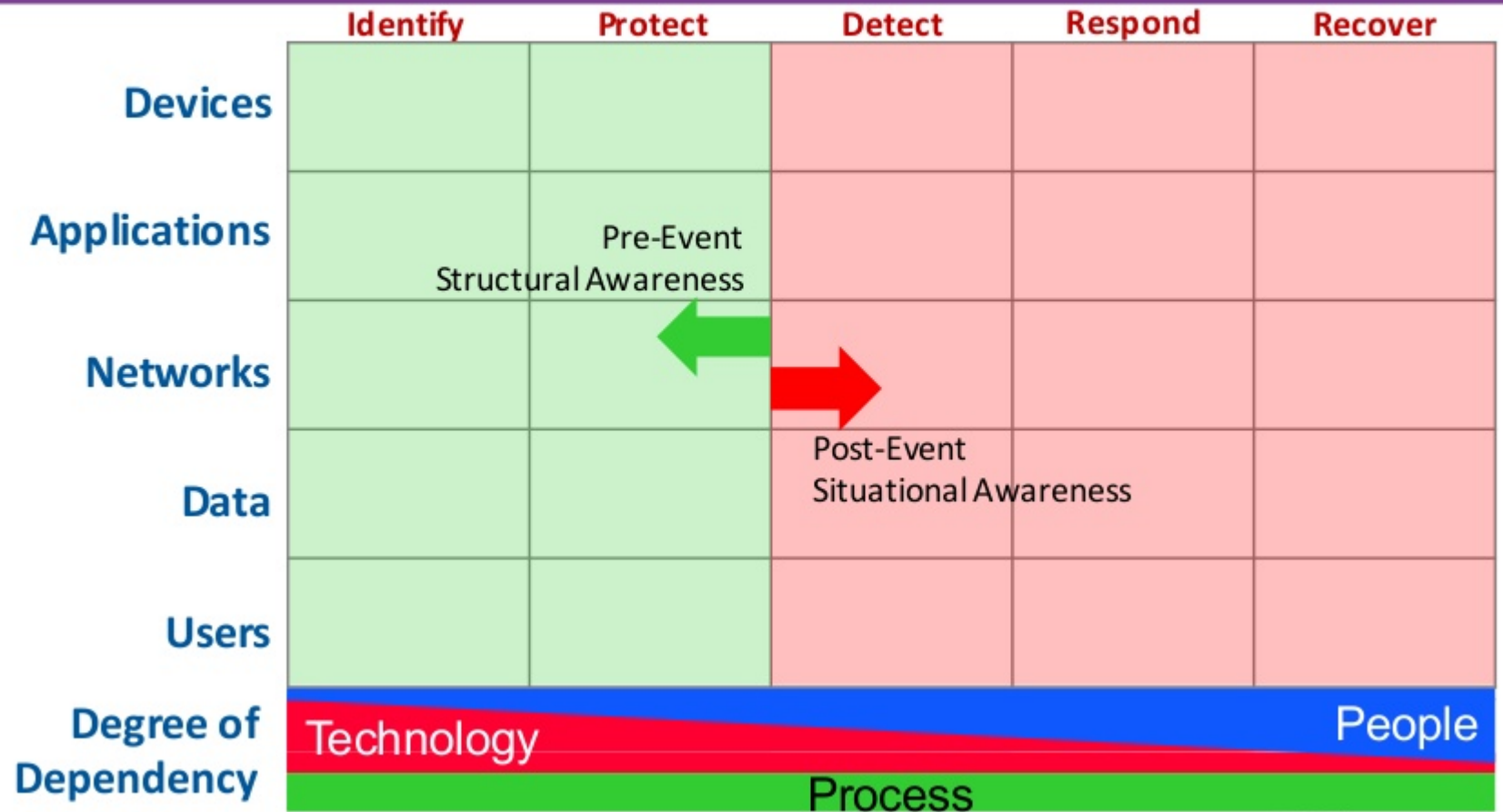
# Introducing the “Cyber Defense Matrix”

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					
Degree of Dependency	Technology				
	Process				
	People				

# Left and Right of "Boom"



#RSAC



# Our common language can be bounded by five asset classes and the NIST Cybersecurity Framework



#RSAC

## Asset Classes

### DEVICES



Workstations, servers, VoIP phones, tablets, IoT, storage, network devices, infrastructure, etc.

### APPS



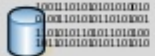
The software, interactions, and application flows on the devices

### NETWORKS



The connections and traffic flowing among devices and applications

### DATA



The information residing on, traveling through, or processed by the resources above

### USERS



The people using the resources listed above

## Operational Functions

### IDENTIFY



Inventorizing assets and vulns, measuring attack surface, baselining normal, risk profiling

### PROTECT



Preventing or limiting impact, patching, containing, isolating, hardening, managing access, vuln remediation

### DETECT



Discovering events, triggering on anomalies, hunting for intrusions, security analytics

### RESPOND



Acting on events, eradicating intrusion footholds, assessing damage, coordinating, reconstructing events forensically

### RECOVER



Returning to normal operations, restoring services, documenting lessons learned





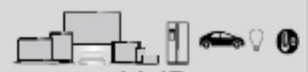
# Enterprise Security Market Segments

	Identify	Protect	Detect	Respond	Recover
Devices		IAM AV, HIPS	Endpoint Visibility and Control / Endpoint Threat Detection & Response		
Applications	Configuration and Systems Management	App Sec (SAST, DAST, IAST, RASP), WAFs			
Networks	Netflow	Network Security (FW, IPS)	DDoS Mitigation IDS		Full PCAP
Data	Data Labeling	Data Encryption, DLP	Deep Web, Brian Krebs, FBI	DRM	Backup
Users	Phishing Simulations	Phishing Awareness	Insider Threat / Behavioral Analytics		
Degree of Dependency	Technology			People	
	Process				



# Security Technologies Mapped by Asset Class

## DEVICES



Workstations, servers, VoIP phones, tablets, IoT, storage, network devices, infrastructure, etc.



## APPS



The software, interactions, and application flows on the devices



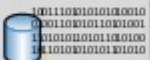
## NETWORKS



The connections and traffic flowing among devices and applications



## DATA



The information residing on, traveling through, or processed by the resources above



## USERS



The people using the resources listed above



Disclaimer: Vendors shown are representative only. No usage or endorsement should be construed because they are shown here.

# Security Technologies Mapped by Operational Functions



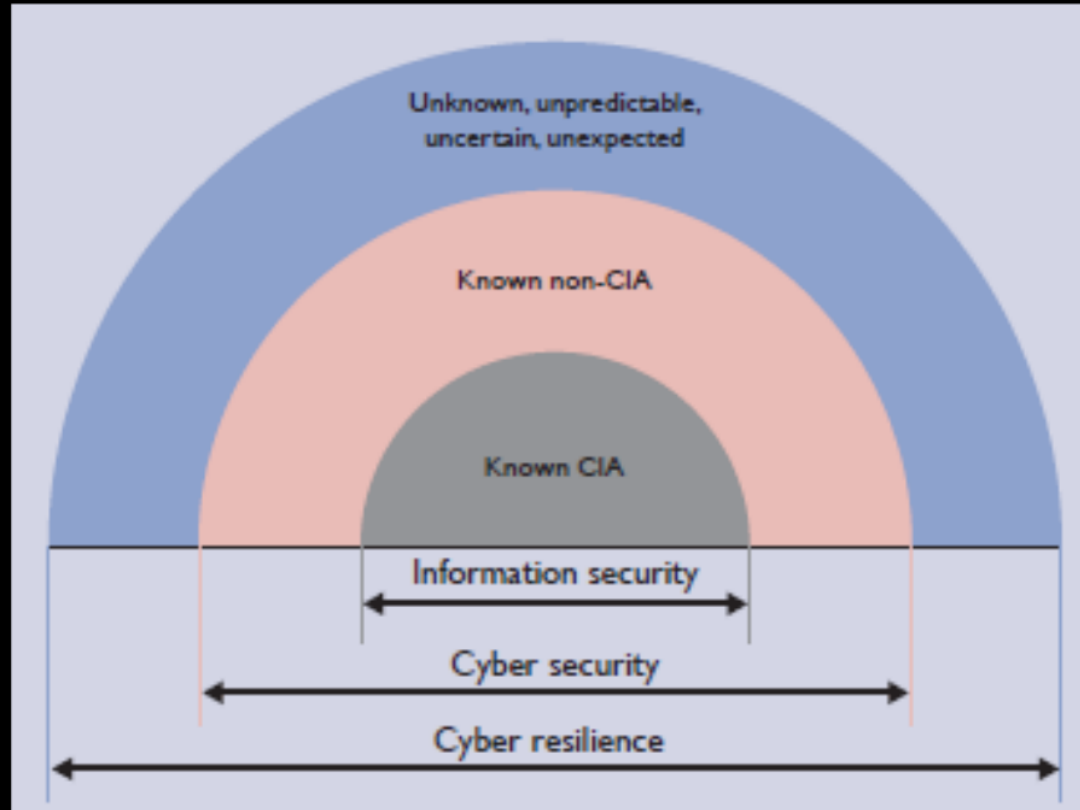
<p><b>IDENTIFY</b></p> <p>Inventorizing assets, measuring attack surface, baselining normal, risk profiling</p>	
<p><b>PROTECT</b></p> <p>Preventing or limiting impact, containing, hardening, managing access</p>	
<p><b>DETECT</b></p> <p>Discovering events, triggering on anomalies, hunting for intrusions</p>	
<p><b>RESPOND</b></p> <p>Acting on events, eradicating intrusion footholds, assessing damage, coordinating, reconstructing events forensically</p>	<div data-bbox="1340 729 1755 958" style="border: 1px solid gray; border-radius: 50%; padding: 10px; text-align: center;"> <p>MSSPs / IR</p> </div>
<p><b>RECOVER</b></p> <p>Returning to normal operations, restoring services, documenting lessons learned</p>	<p>VERITAS</p>

Disclaimer: Vendors shown are representative only. No usage or endorsement should be construed because they are shown here.





# As we're meant to be resilient now



Source: ISF - Cyber Security Strategies

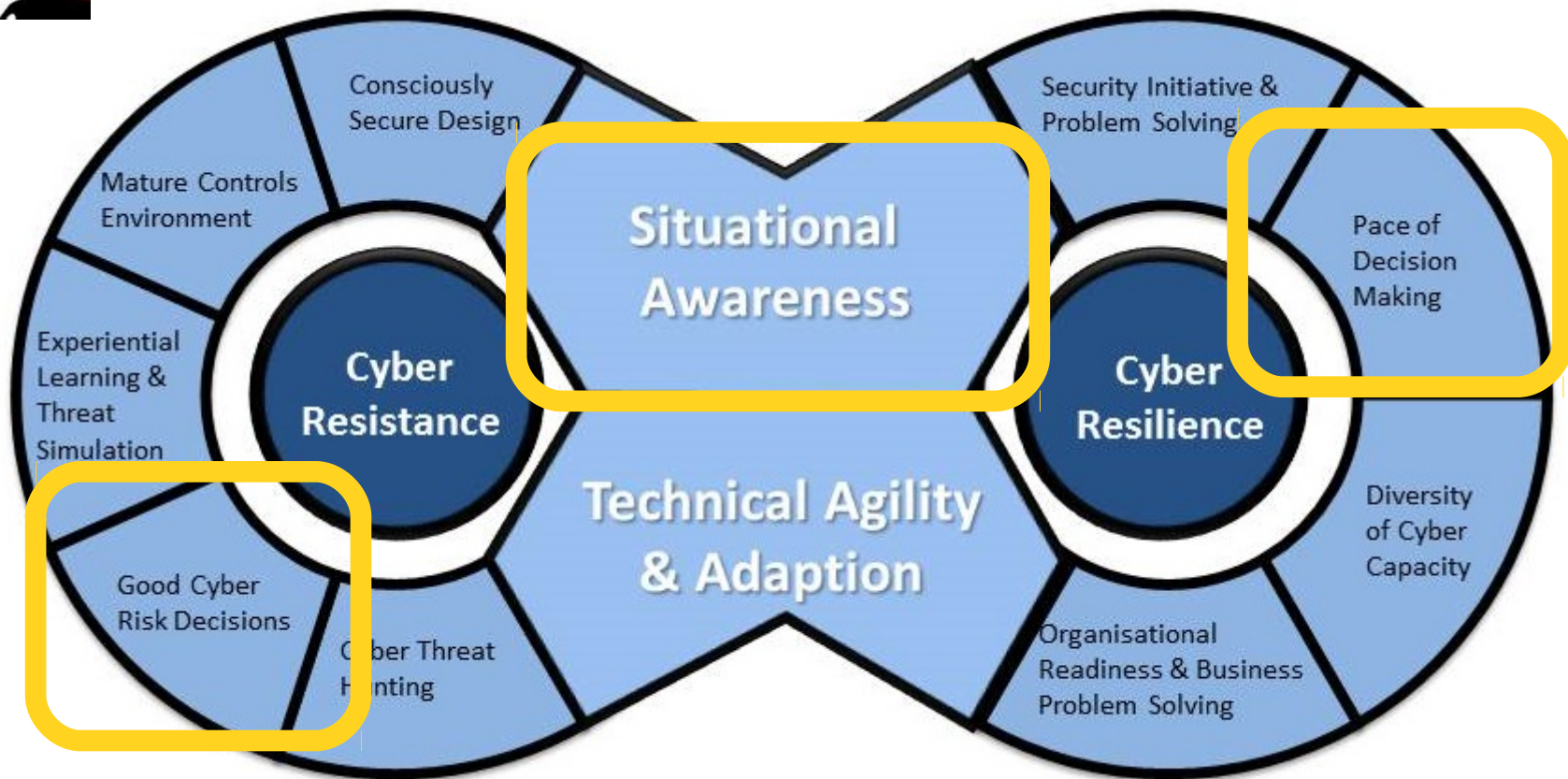


# NCSC - “Cyber resilience - nothing to sneeze at”





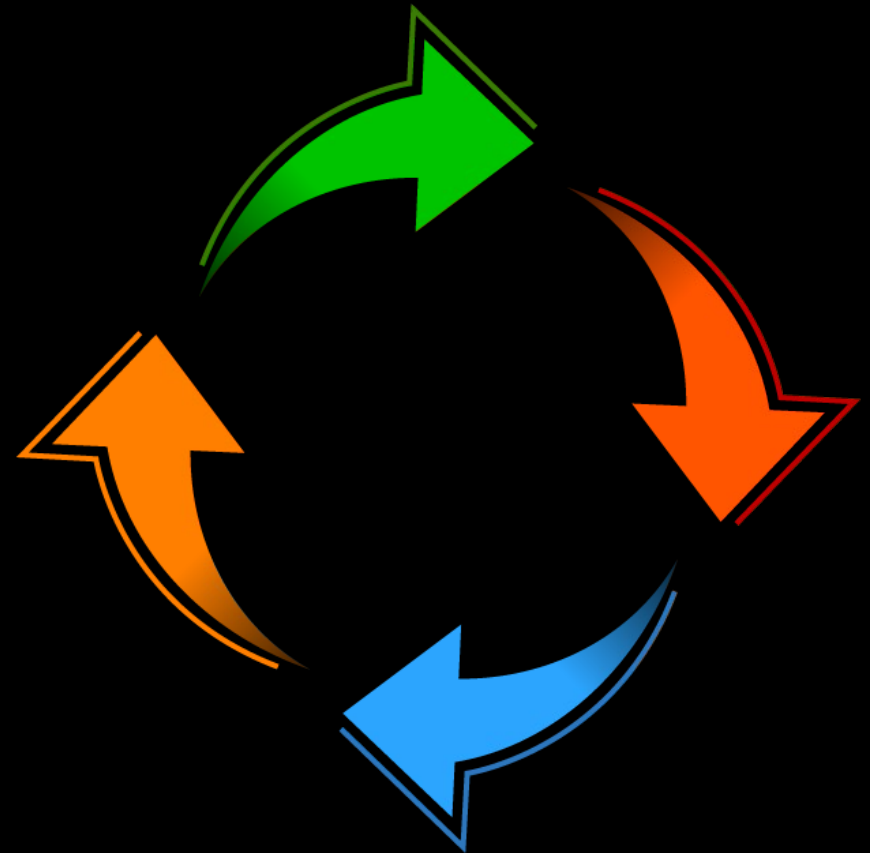
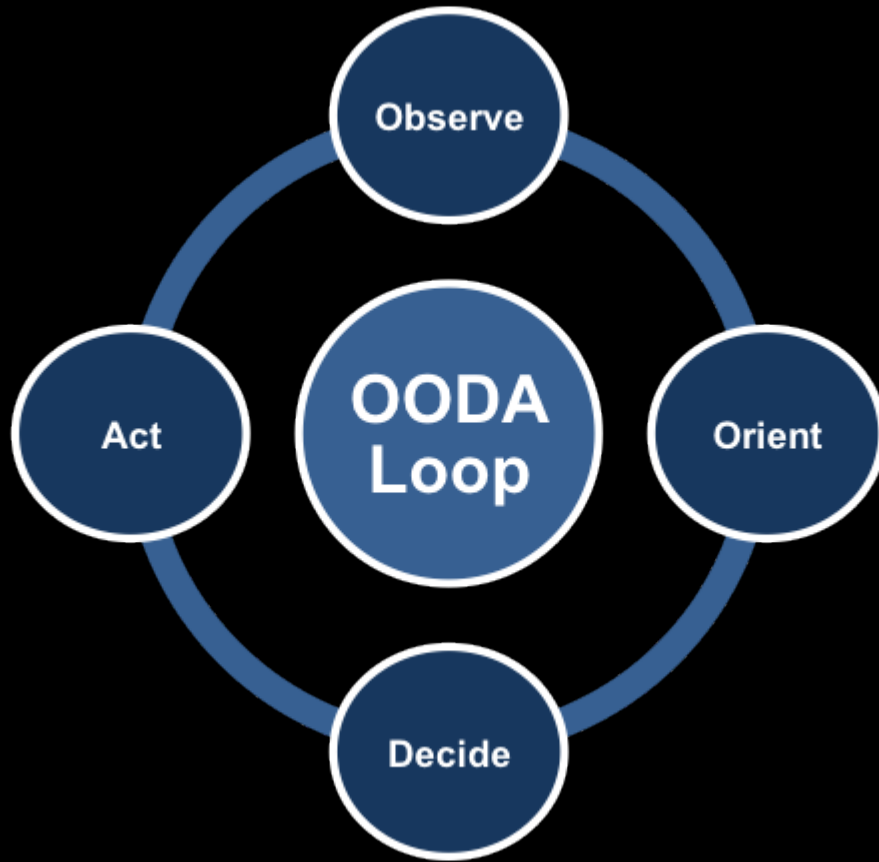
# Blog - Black Swan Security

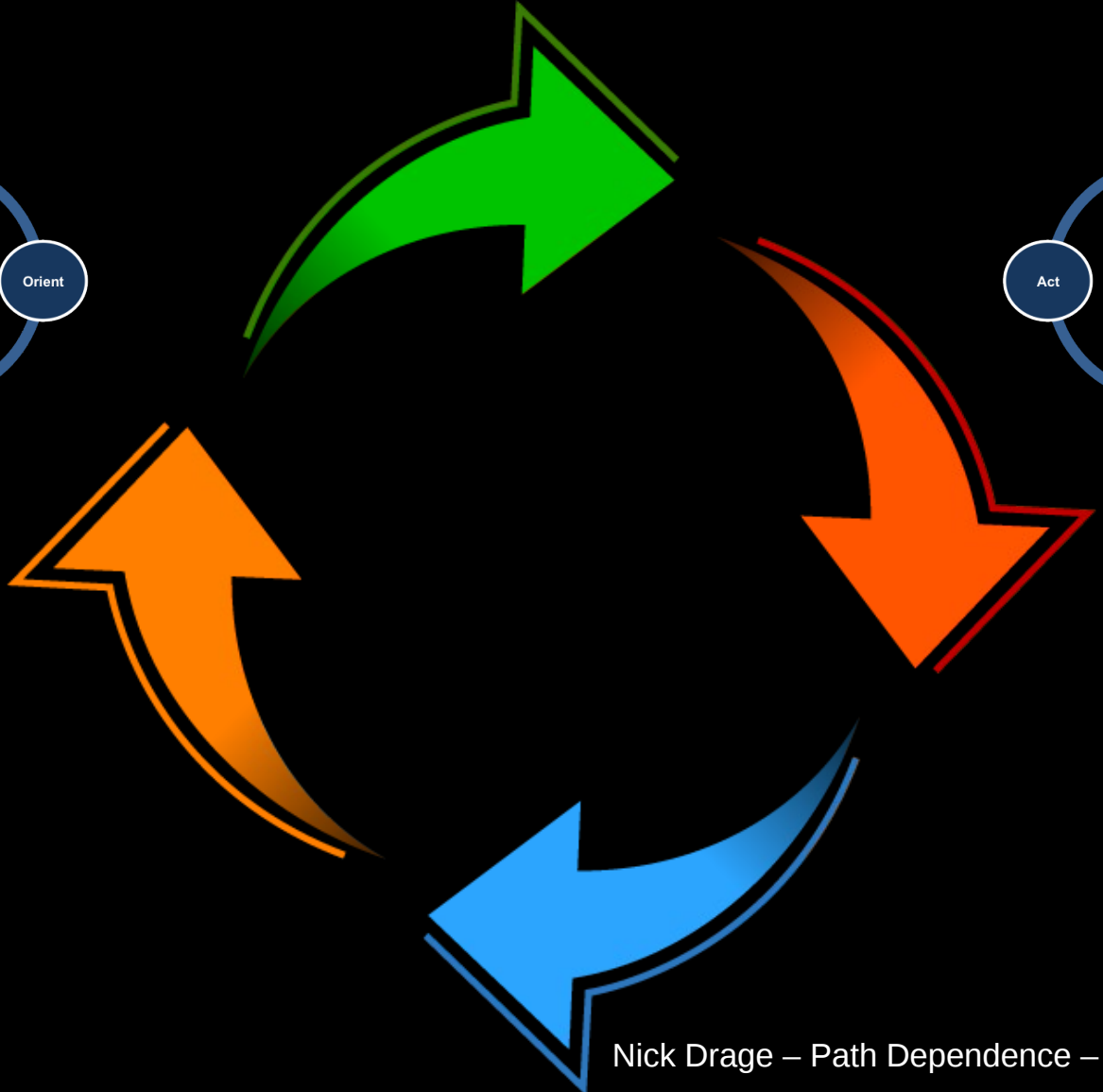
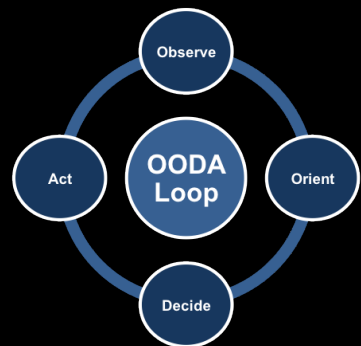
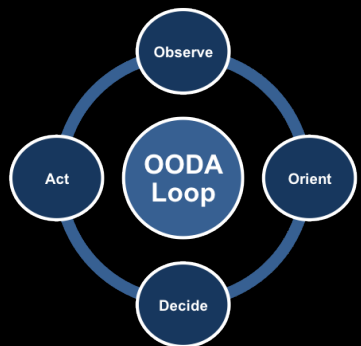




Nick Drage – Path Dependence – @SonOfSunTzu

# OODA: Observe – Orient – Decide - Act

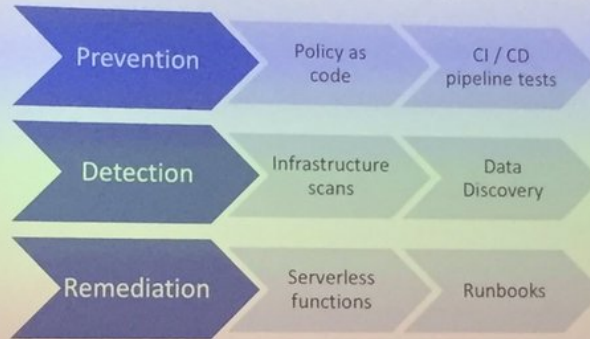






DevSecCon

### Continuous Cloud Compliance Framework



Making continuous development

DevSecCon

DevSecCon

The DevSecCon conference

Image: Mark Skillen

# LESSON – out hit your opponent

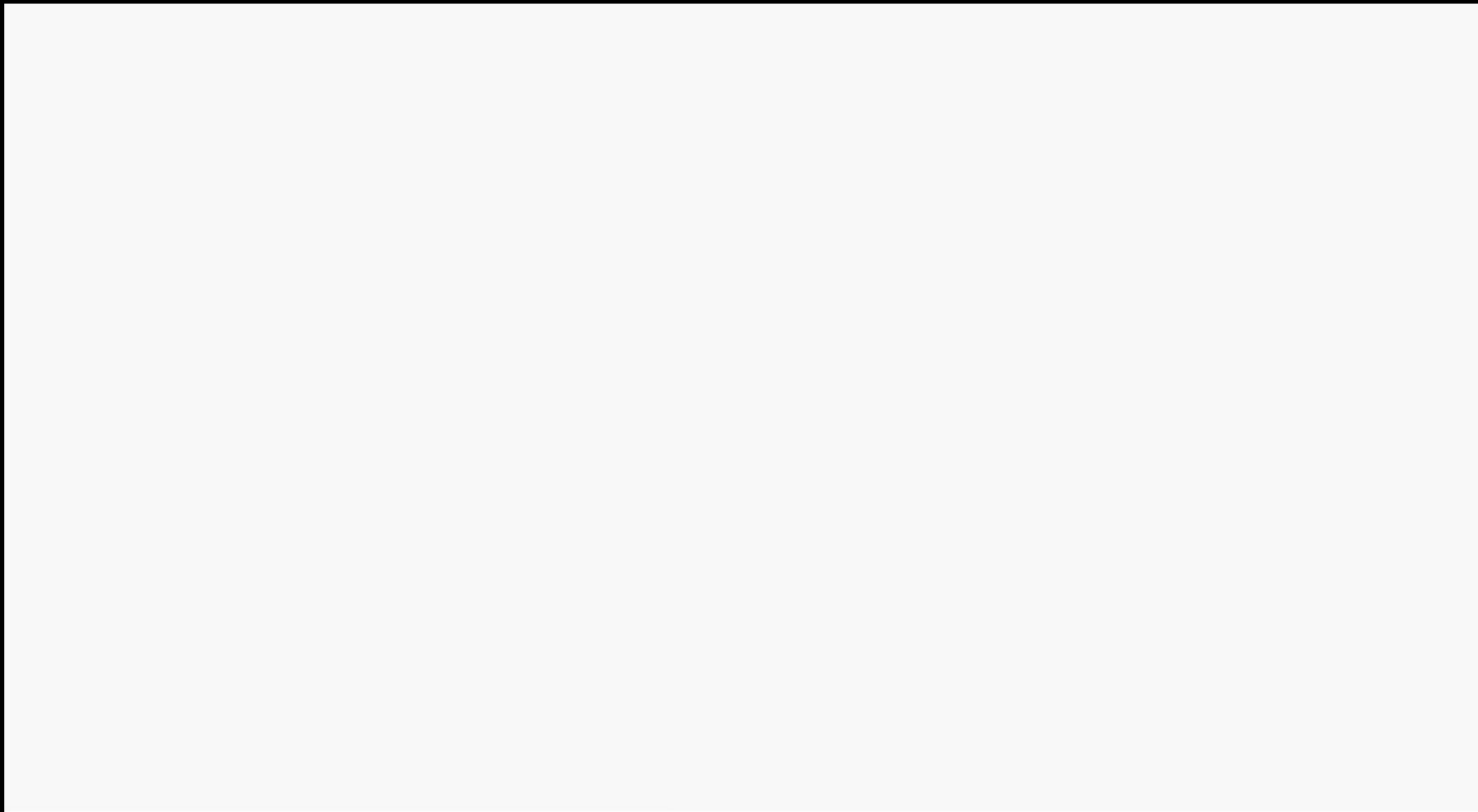
## *Content of Models*

- *Phenomena Omitted or Buried.* Typically, ground-combat simulations focus on complex calculations of attrition while treating command-control processes, tactics, and strategy in terms of stereotypes embedded in the data bases. This ignores the evidence of history that such matters (and other “soft factors”) are first-order determinants of both deterrence and war outcomes, and should therefore be highlighted.<sup>12</sup>

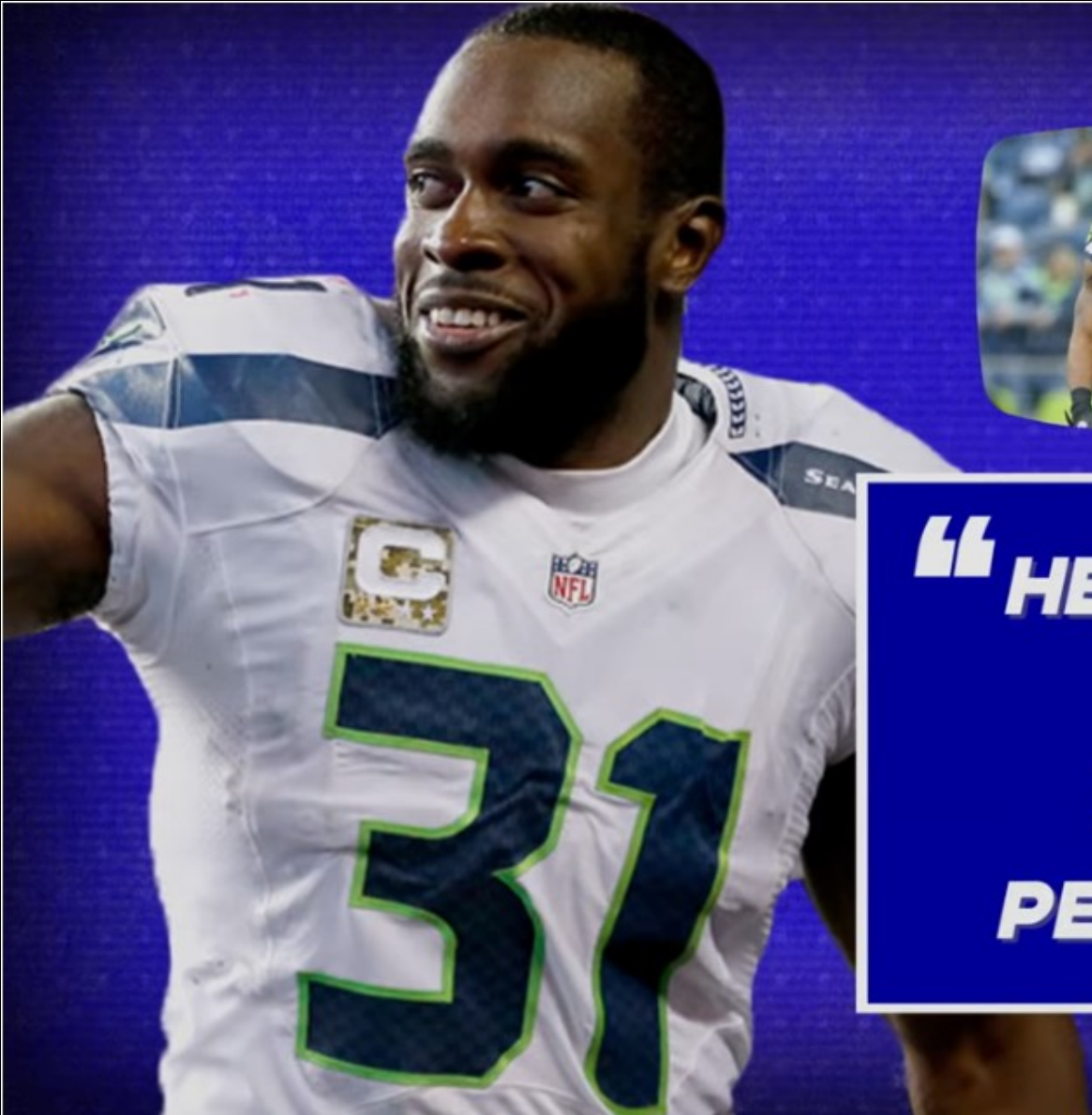
The evidence of history is that soft factors: command-control processes, tactics, and strategy, are first-order determinants of both deterrence and war outcomes ( emphasis mine )

THE LEGION OF  
**BOOM**





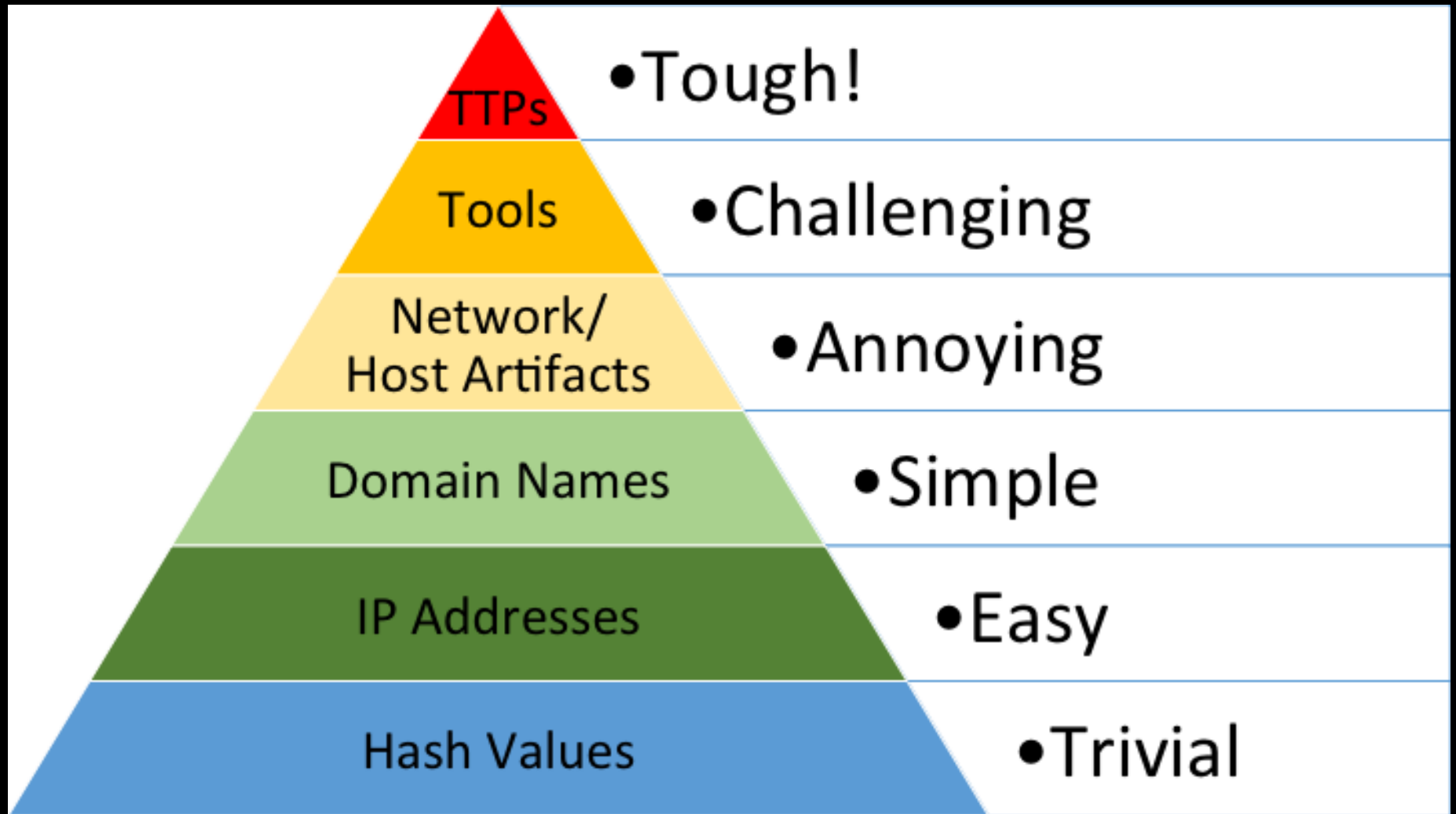




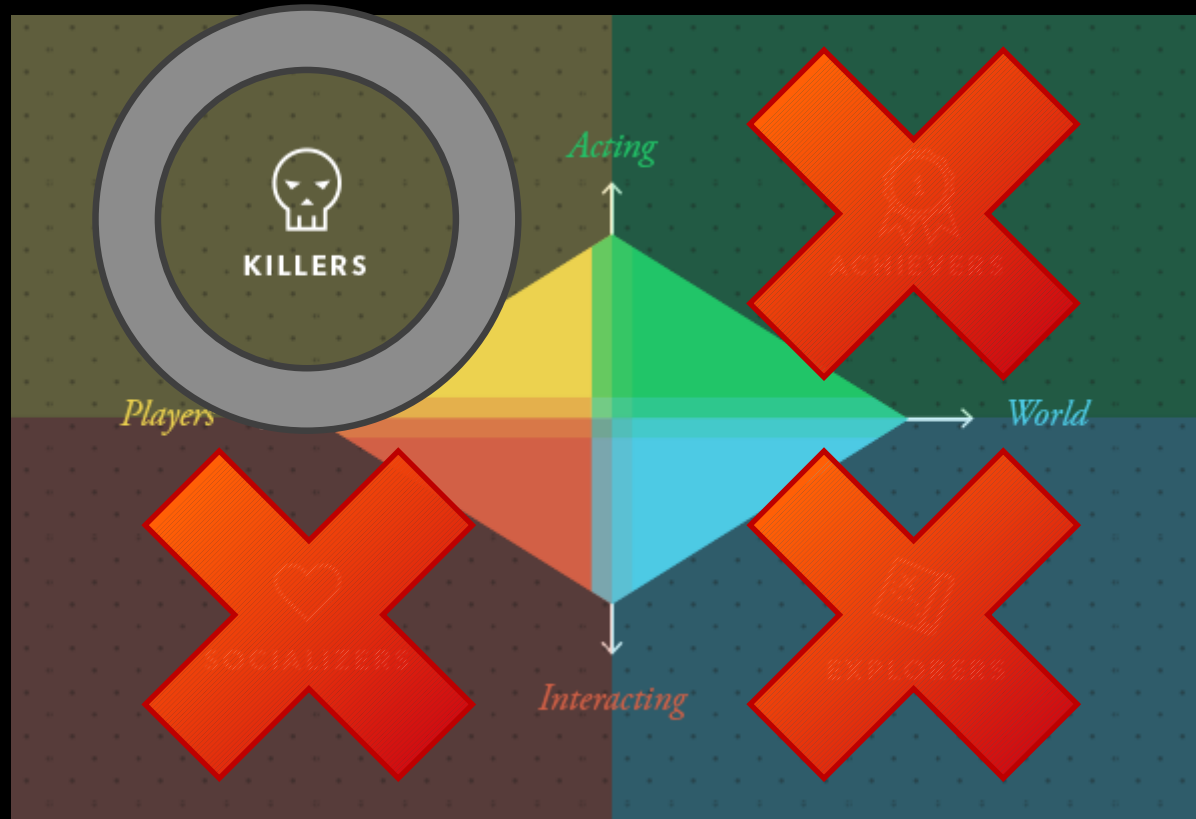
## **RICHARD SHERMAN**

**“HE’S A FREAKING  
MONSTER.  
HE DAMAGES  
PEOPLE’S SOULS.”**



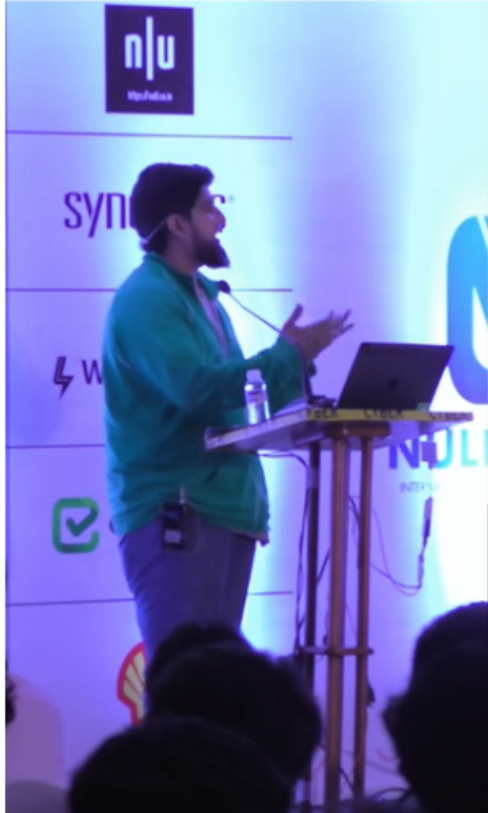


# Bartle's Taxonomy of Player Types





**NULLCON**  
INTERNATIONAL SECURITY CONFERENCE



# HACK

MAKE DEFENSE GREAT AGAIN!

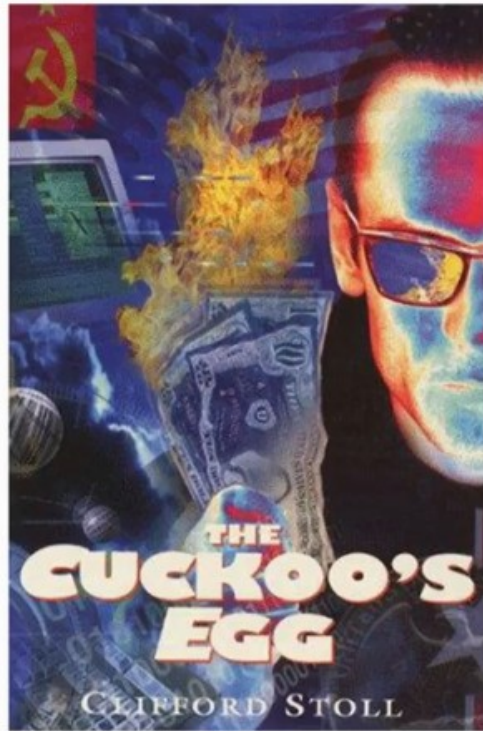


**Making A Dent, Making A Difference  
And Making A Dollar  
- Haroon Meer**



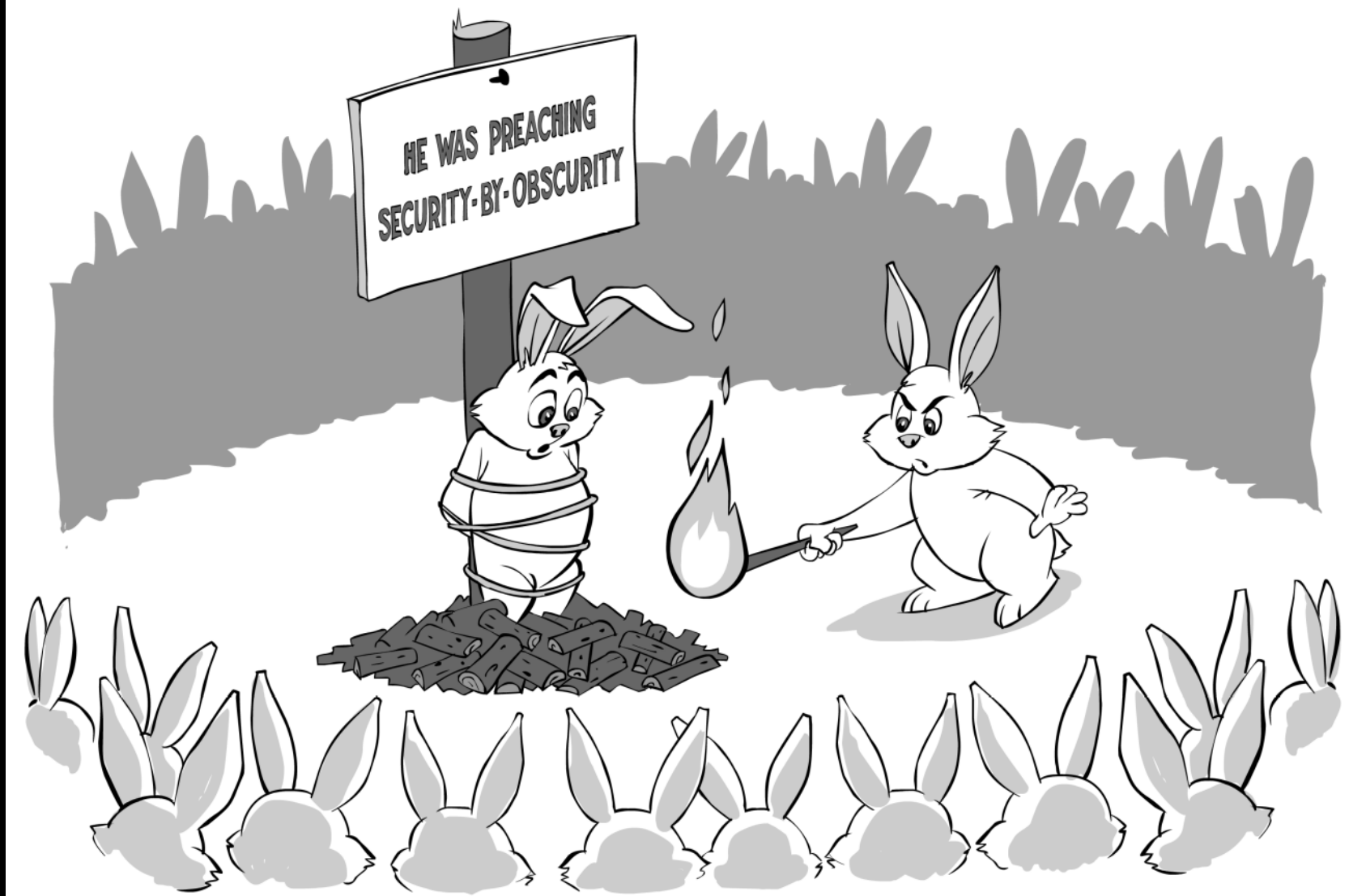
Image: Yan Cui

people are often the **WEAKEST** link  
in the security chain



# Everything You Know Is Wrong - Paul Midian







**blackhat**  
ASIA 2017

**blackhat**<sup>®</sup>  
ASIA 2017

The Seven Axioms  
of Security

BLACK HAT BRIEFINGS AND TRAININGS  
TRAINER  
BLACK HAT USA 2016

The Black Hat Briefings  
1999

SAUMIL SHAH  
CEO, NET SQUARE  
@therealsaumil

BLACKHAT ASIA - SINGAPORE 2017

NETSQUARE

Keynote: The Seven Axioms of Security

# Seven Axioms of Security: 6

The Best Defense  
is a **CREATIVE**  
**Defense.**





DevSecCon

DevSecCon

The  
DevSecOps  
conference  
Making continuous security  
a reality

```
resource "aws_s3_bucket" "app" {
  count = "${var.create_app ? 1 : 0}"
  bucket = "${var.name}-${var.hash}"
  acl = "private"
  website {
    index_document = "index.html"
    error_document = "index.html"
  }
  tags = {
    "Environment": "2008-10-17",
    "Statement": 1
  }
  policy = jsonencode({
    "Statement": [
      {
        "Sid": "PublicReadForciblyBucketObjects",
        "Effect": "Allow",
        "Principal": "*",
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::${var.name}-${var.domain}/*"
      }
    ]
  })
}

lifecycle {
  prevent_destroy = true
}

tags {
  "relatio" = "apps"
}

resource "aws_s3_bucket" "next_app" {
  count = "${var.create_app ? 1 : 0}"
  bucket = "${var.name}-${var.domain}"
  acl = "private"
  website {
    index_document = "index.html"
    error_document = "index.html"
  }
}
```

## Dark Nets

Image: Meadow Ellis



Image: DevSecCon

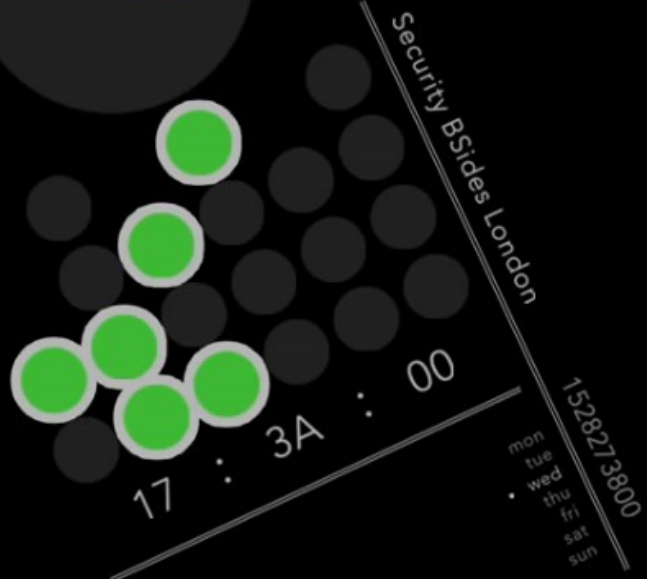




# SOLVING THREAT DETECTION

6<sup>th</sup> June 2018

COUNTERCEPT



## Defender's Dilemma

The intruder only needs to exploit one of the victims in order to compromise the enterprise.

## Intruder's Dilemma

The defender only needs to detect one of the indicators of the intruder's presence to initiate incident response within the enterprise.

Richard Bejtlich - <https://taosecurity.blogspot.de/2009/05/defenders-dilemma-and-intruders-dilemma.html>




**Att&ck™ The Attacker**  
**- Christian Kollee**

# GASLIGHTING WITH HONEYPITS AND MIRAGES

DESTROYING DISCOVERY TO DEplete ATTACKERS

Catherine (Kate) Pearce

*Sr. Security Consultant, Cisco Security Services*



“Never attempt to win by force what can be won by deception.”

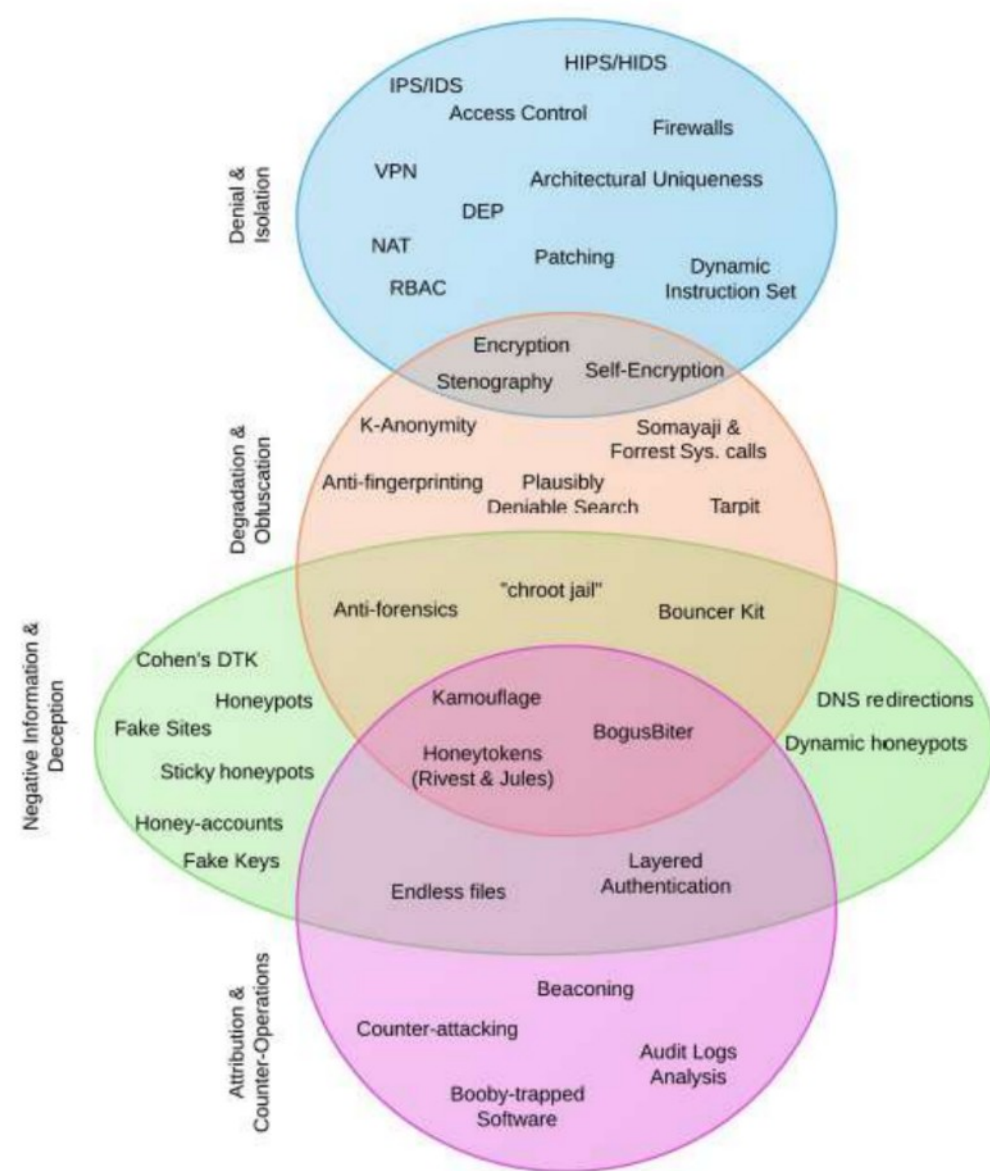
Niccolò Machiavelli,

*The Prince*



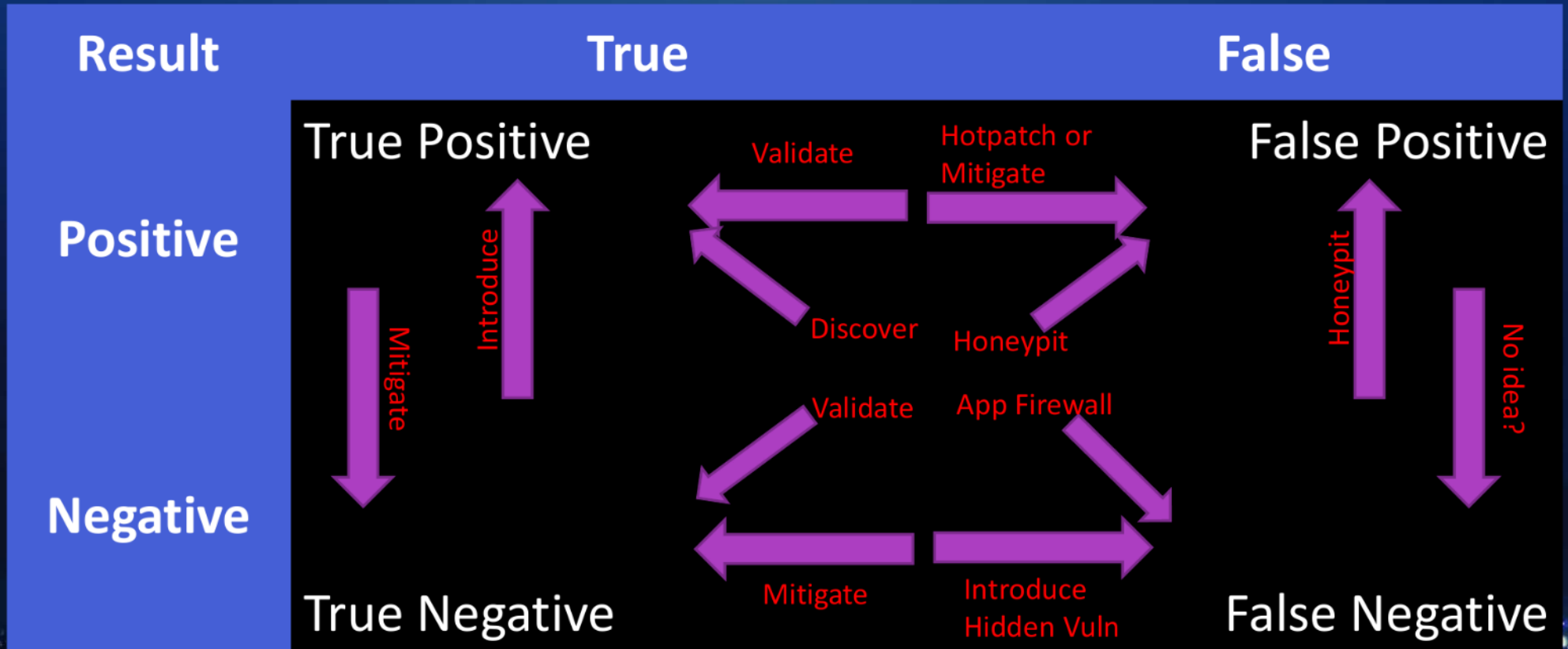
# DECEPTION EXAMPLES – INFORMATION SECURITY

- From Almeshekah





# POSSIBILITIES - TRANSITIONS



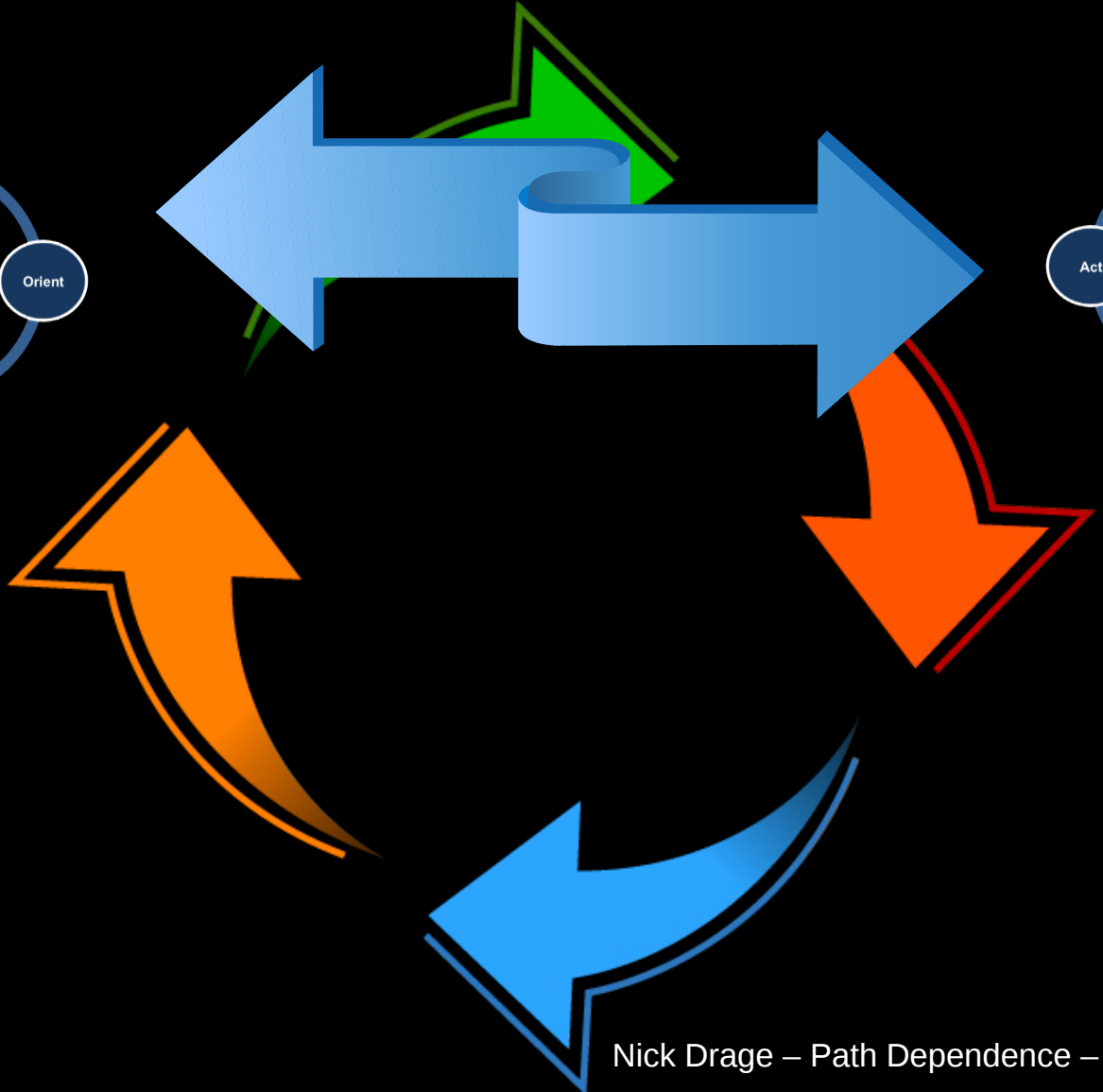
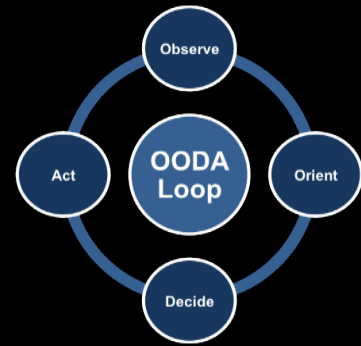
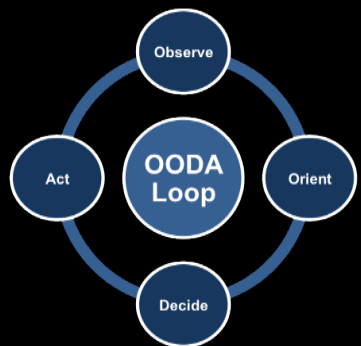
# TRANSIENT PROBLEMS – MISSPEAKING

## ANSWER PRETTY MUCH AS EXPECTED BUT NOT QUITE

- Random errors
  - Random timing errors
  - Random omissions
  - Random bitflips
  - Random endian changes
  - Random number changes
  - Badly signed things
  - Badly encrypted things
  - Random wrong content
- Nonrandom errors to break things
  - Invalid characters/bytes
  - Terminal command characters
  - Random “unallocated” memory
  - Bad pointer values
  - Filesystems of the wrong type
  - Impossible filenames
  - Timing “errors”
  - “Omissions”

# GASLIGHTING - MORE

- Uncrackable Hashes
- Decoy Systems, Ports, Services
- Manufactured Vuln Emulation
  - E.g. MS08-067?
- Decoy Vulns (static)
- Decoy Vulns (non exploitable {buffer overflow in managed lang})
- Nondeterministic Existence
- For you only existence
- Transient Vulns
- Transient Systems, Ports, Services
- Vuln neutering
- Vuln Chains leading nowhere
- Benign Passthrough
- Honeypot Passthrough
- Trickster passthrough
- One time Vulnerability Generation
- One time vulns as canaries
- Answering questions you never asked
- Answering different questions
- Fake answers
- Fake Data
- Silent Failure (denying you ever agreed)
- Rewriting page format dynamically to break validation and cscripting



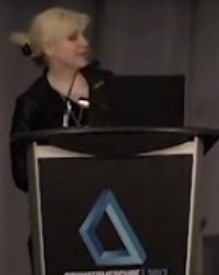
# CHANGE CONTROL?





# The Red Pill of Resilience

Kelly Shortridge (@swagitda\_)  
COUNTERMEASURE 2017



A close-up photograph of a monkey's face, focusing on the eye and nose area. The monkey has dark brown fur and a prominent red face. The text "Chaos Monkey" is overlaid in white, centered on the face.

Chaos Monkey

Randomly kills instances to test their ability to withstand failure.

It also makes persistence really hard.

# RSA<sup>®</sup>Conference2017

San Francisco | February 13-17 | Moscone Center

POWER OF  
OPPORTUNITY

SESSION ID: MASH-F02

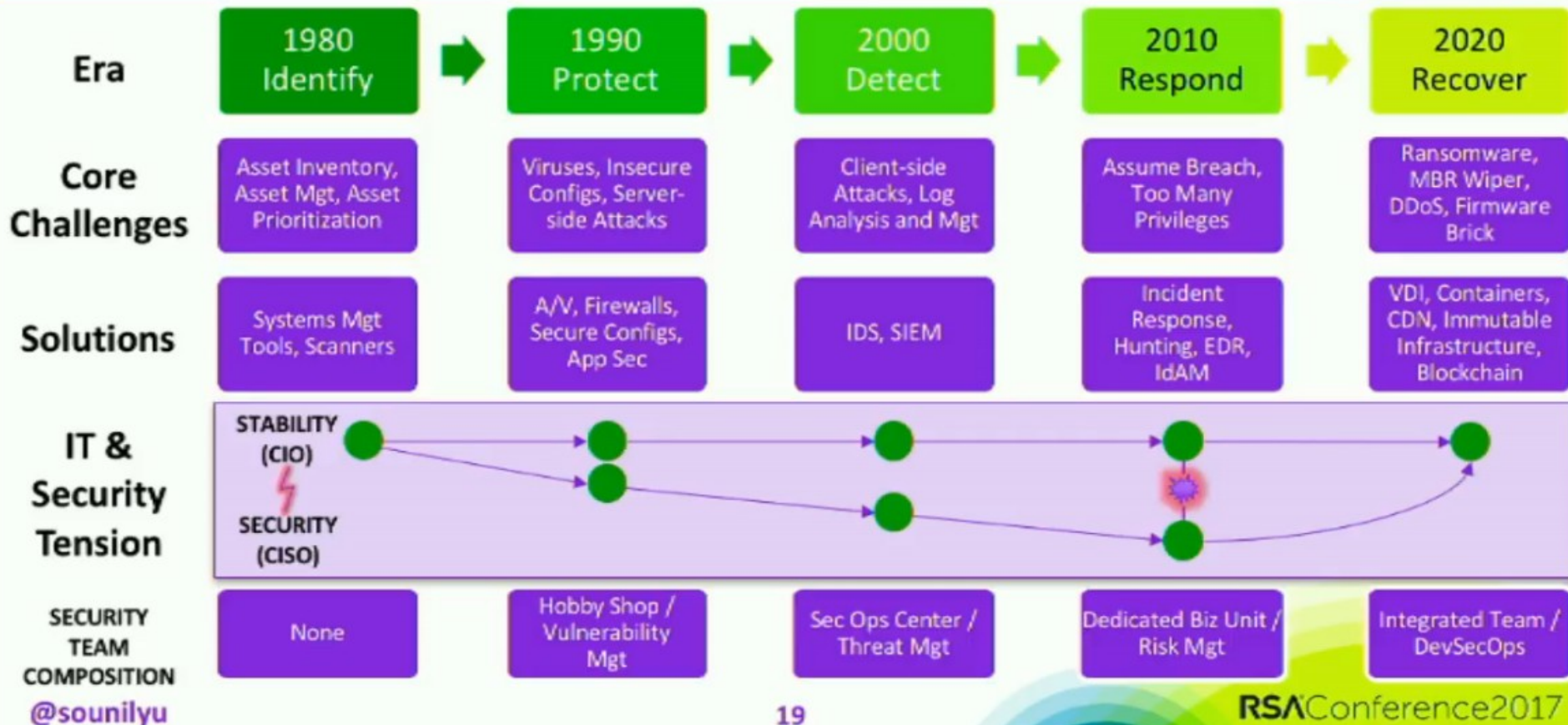
## Solving Cybersecurity in the Next Five Years Systematizing Progress for the Short Term



Sounil Yu  
@sounilyu



# Mapping to the NIST Cyber Security Framework



@sounilyu

19

RSAConference2017

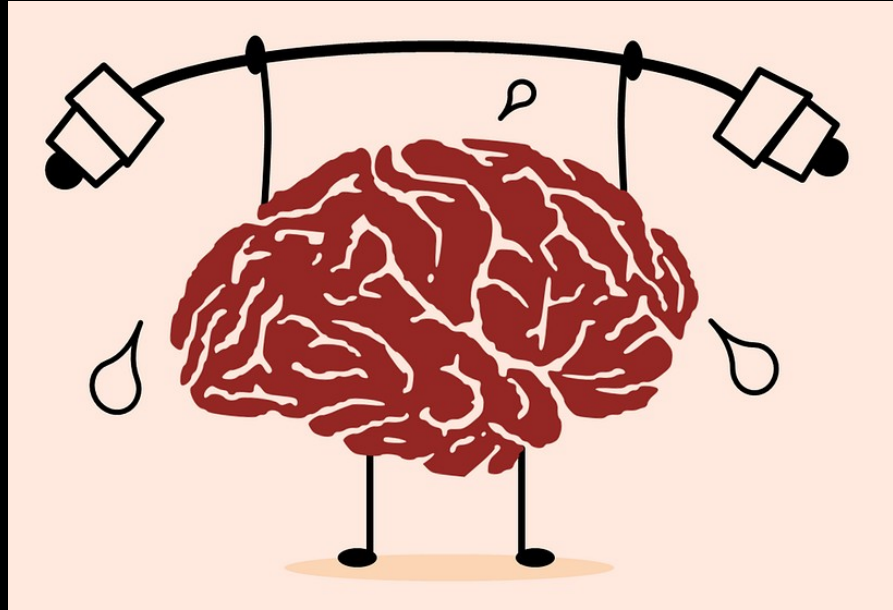
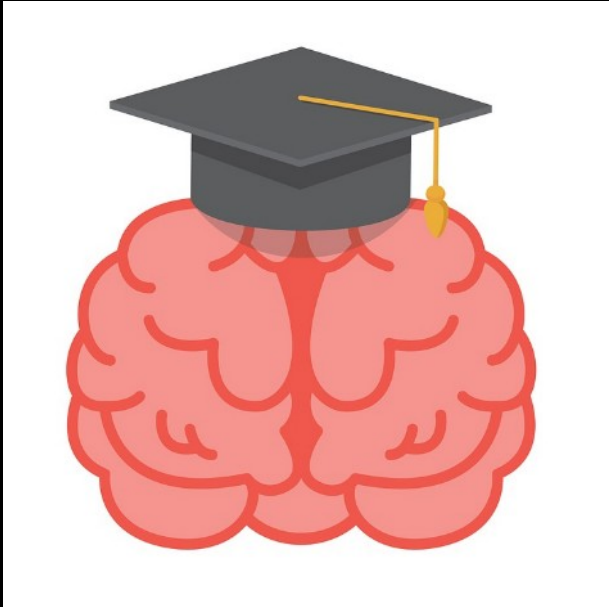


Not a blinky  
box you can  
buy, install  
and ignore



**Agile is not  
a thing you buy.**

**Agile is  
a thing you are.**





**Sunny Bear - Sun Tzu**

@Sunni\_Tzu

Follow



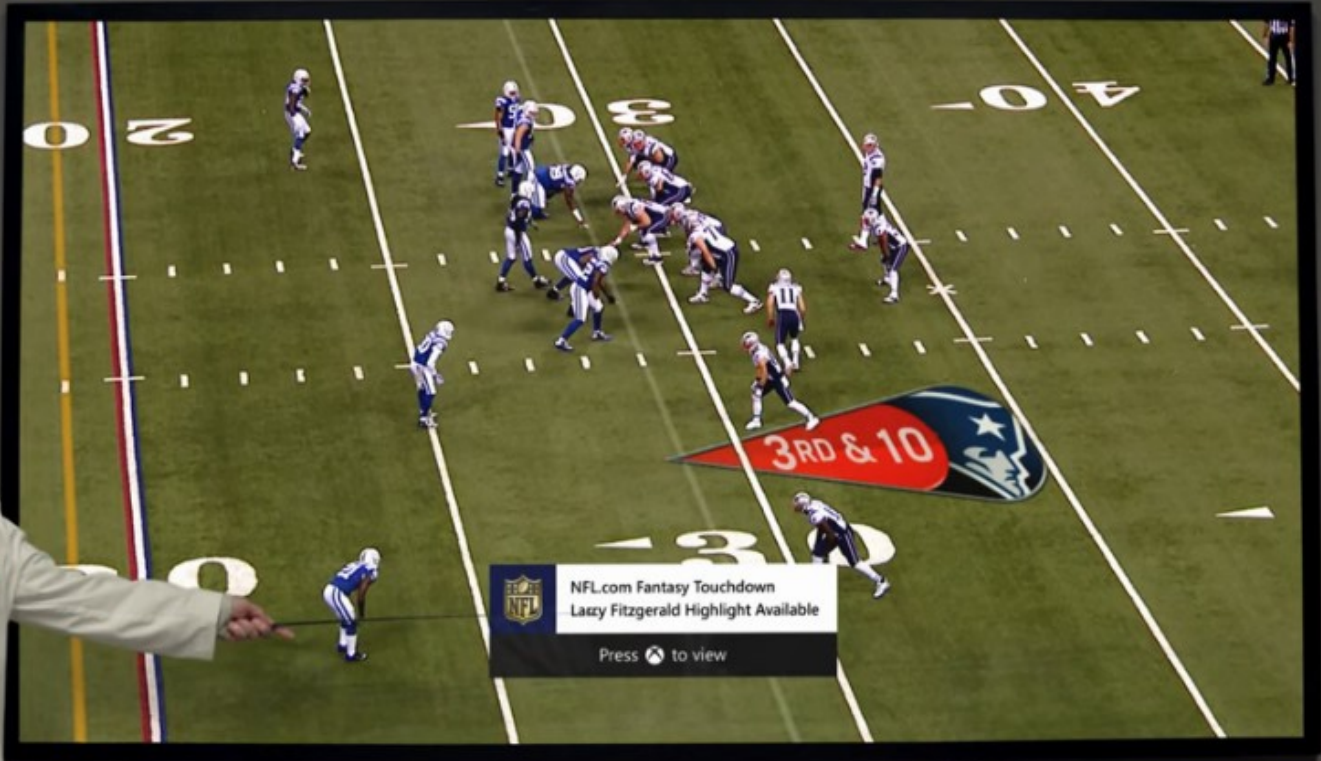
Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.

[#SunTzu](#)



Nick Drage – Path Dependence – @SonOfSunTzu





NFL.com Fantasy Touchdown  
Lazy Fitzgerald Highlight Available  
Press [Xbox button] to view

Screens simulated; subject to change.







# LESSONS

- Use others' lessons
- Practice Is Everything
- Eliminate the Big Play
- Out Hit Your Opponent
- Or try to Golf our way through American Football...



Nick Drage – Path Dependence – @SonOfSunTzu



Nick Drage – Path Dependence – @SonOfSunTzu



DevSecCon

[Nick Drage

[nickd@pathdependence.co.uk](mailto:nickd@pathdependence.co.uk)

[blog.sonofsuntzu.org.uk](http://blog.sonofsuntzu.org.uk)

@SonofSunTzu]



LONDON 18-19 OCT  
2018

BREAK BREAK BREAK